

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年4月15日 (15.04.2004)

PCT

(10) 国際公開番号
WO 2004/031941 A1

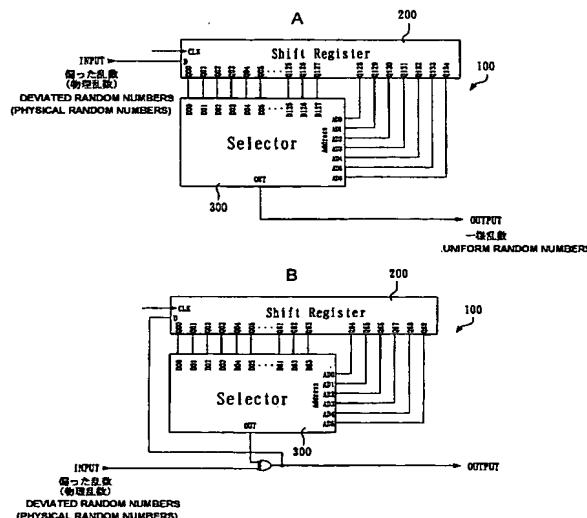
- (51) 国際特許分類: G06F 7/58
- (21) 国際出願番号: PCT/JP2003/012213
- (22) 国際出願日: 2003年9月25日 (25.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-285168 2002年9月30日 (30.09.2002) JP
特願2003-101085 2003年4月4日 (04.04.2003) JP
特願2003-294101 2003年8月18日 (18.08.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): FDK 株式会社 (FDK CORPORATION) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 山本 博康 (YAMAMOTO, Hiroyasu) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). ビターナゲ アナンダ (VITHANAGE, Ananda)

[LK/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 清水 隆邦 (SHIMIZU, Takakuni) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 藤田 香 (FUJITA, Kaoru) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 中野 初美 (NAKANO, Hatsumi) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 志賀 隆明 (SHIGA, Takaaki) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 曾我 竜司 (SOGA, Ryuji) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 上遠野 昌良 (KATONO, Masayoshi) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 渡邊 利幸 (WATANABE, Toshiyuki) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP). 鯉淵 美佐子 (KOIBUCHI, Misako) [JP/JP]; 〒105-0004 東京都港区新橋5丁目36番11号 FDK株式会社内 Tokyo (JP).

[続葉有]

(54) Title: METHOD OF UNIFORMING PHYSICAL RANDOM NUMBER AND PHYSICAL NUMBER GENERATION DEVICE

(54) 発明の名称: 物理乱数の一様化手法と物理乱数発生装置



(57) Abstract: A method of uniforming physical random numbers, capable of maintaining a random number generating velocity and ensuring security concurrently. The method sequentially inputs a plurality of physical random numbers to a shift register to hold them there, and shifts them every time a reference pulse signal rises. Physical random numbers held in the shift register are randomly selected and output by a selector based on part of them. Accordingly, physical random numbers input to the shift register are uniformed and then output even though they have a deviation, thereby eliminating the chance of not outputting random numbers or letting others recognize the deviation of random numbers.

[続葉有]

WO 2004/031941 A1



(74) 代理人: 清水 千春, 外 (SHIMIZU, Chiharu et al.); 〒
104-0061 東京都中央区銀座8丁目16番13号中
銀・城山ビル4階 Tokyo (JP).

添付公開書類:
— 国際調査報告書

(81) 指定国 (国内): CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(57) 要約:

乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供する。本発明によれば、複数の物理乱数をシフトレジスタに順次入力して保持し、基準パルス信号が立ち上がるごとにシフトする。シフトレジスタに保持された物理乱数をその一部に基づいてセレクトでランダムに選択して出力する。これにより、シフトレジスタに入力された物理乱数は、それが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られる事態が起きない。

明 細 書

物理乱数の一様化手法と物理乱数発生装置

5

技 術 分 野

本発明は、偏りのある物理乱数を簡単に一様化することが可能な物理乱数の一様化手法に関するものである。

更に、本発明は、各種の用途に用いるに好適な物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（
15 例えば、CG、自動作曲）、制御、計測、FA、ロボット制御（人工知能）などが挙げられる。

背 景 技 術

一般に乱数には、計算によって決定論的に生成される擬似乱数と、自然界の物理現象を利用して生成される物理乱数とがある。後者（物理乱数）は真の意味でランダムな現象を基に生成されるので、理想的な乱数となる資質があるものの、実際に物理乱数を生成する場合、途中過程で様々な誤差要因が介在するため、必ずしも理想的な乱数が出力されるとは限らず、偏りのある乱数が出てきてしまう恐れもある。この誤差要因としては、デジタル化の際に基準となるクロックの幅
25 や、ノイズを利用する場合に余計なノイズが混入することなどが挙げられる。

従来、こうした物理乱数の偏りを改善する手法、すなわち物理乱数の一様化手法としては、2つの2進乱数を用いて乱数の偏りを改善するノイマンコレクター（例えば、非特許文献1参照）や、ノイズに基づいて発生させた物理乱数を擬似乱数と合成することで物理乱数の偏りを改善する手法（以下、乱数合成法と称す

る。)が提案されていた(例えば、特開2001-344094号公報(段落
〔0014〕および〔0018〕の欄および図1参照、また、非特許文献である
Benjamin Jun and Paul Kocher著、"The Intel Random Number Generator"、CRY
PTOGRAPHY RESEARCH、1999年4月22日発表(第4頁、4.3.Digital Post-P
5 rocessing)参照。)

しかし、ノイマンコレクターでは、1ビットの乱数を出力するのに2ビットの
乱数を必要とする上に、その2ビットの組合せによっては乱数を出力しない場合
もあるので、乱数の発生速度が落ちてしまう欠点があった。

また、乱数合成法では、擬似乱数がわかれば、基になる物理乱数を出力から取
10 り出せるようになるため、乱数の偏りが他人に知られてしまい、保安性に欠ける
という不都合があった。

また、前記したような従来の物理乱数発生装置としては、半導体内で発生する
ノイズを用いたものが多く、パソコンに外部から接続して使用するよう構成され
る規模の大きなものや、ICチップ単体で乱数を発生させるものがあった。また
15 、アミューズメント用には、時間的にランダムであると見なせる信号が発生した
時に、備えられた高速カウンターの値を参照し、それを乱数として用いるものが
あった。

一般に物理乱数発生器は高速に乱数を発生することは難しく、時としてその乱
数発生速度以上の大量の乱数が必要となる事が起こる。そのため、記憶媒体を設
20 けて乱数を貯めておいたり、複数の物理乱数発生装置を用いで乱数の発生量を増
やしたりすることが考えられるが、これを実現するためには複雑な回路を利用者
側で組む必要が生じる。

また、一般に物理乱数は使用環境によって乱数の質が変化する可能性があり、
利用者がこれら物理乱数発生装置の発生した乱数が真正乱数として使用すること
25 ができるか否かを確認することは有益なことである。しかしながら、乱数の検定
を行うには専用の測定装置を構築しなければならず、一般の物理乱数発生装置利
用者にとっては、このような余計なコストと手間がかかるような作業は受け入れ
難い。また、乱数検定は大量のデータを扱うので、それを貯めておく記憶装置は
大容量のものが必要となるとともに、検定のための計算処理にも時間がかかる。

更に、従来の物理乱数発生装置としては、例えば特開 2003-29964 号公報に開示されているように、2 個のディレーおよびセレクター等からなる位相調整部と、フリップ・フロップと、フィードバック回路とから構成される物理乱数発生器を備えたものが知られている。

- 5 しかし、これでは、フリップ・フロップのクロック端子とデータ端子に入力される 2 系統の信号ラインに応じた 2 個のディレーおよびセレクターが必要となるので、位相調整部、ひいては物理乱数発生器の規模が大きくなり、その占有面積が拡大するばかりか、その消費電力が増大するという不都合があった。特に、物理乱数発生器が CPU（中央演算処理装置）、ROM（読取り専用記憶装置）、RAM（読取り書き込み記憶装置）などの多くの機能と IC（集積回路）内に混載
10 される場合には、この物理乱数発生器の専有面積をできる限り縮小することが強く望まれる。

発 明 の 開 示

- 15 本発明は、このような事情に鑑み、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することを目的とする。

- 本発明の他の目的は、物理乱数発生装置単体での乱数利用効率が高く、かつ複数の物理乱数 IC を組み上げて乱数を高速に発生させることが容易であり、さらに、乱数の質を容易に確認して使用することが可能な物理乱数発生装置を提供せ
20 んとするものである。

更に、本発明の別の目的は、占有面積が小さくて消費電力が少ない物理乱数発生器と、この物理乱数発生器が組み込まれた物理乱数発生装置を提供せんとするものである。

- 25 先ず、本発明のうち、請求項 1 に係る発明は、複数の物理乱数を乱数保持装置（200）に入力して保持し、この乱数保持装置に保持された物理乱数の一部をセレクターのアドレスとして使用し、そのアドレスに基づいて残りの部分から乱数をランダムに選択して出力することを特徴とする物理乱数の一様化手法である。

また、本発明の請求項 2 に係る発明は、前記セレクターに代え、論理積回路を

用い乱数保持装置に保持された乱数をランダムに選択して、それらの排他的論理和を出力することを特徴とする物理乱数の一様化手法である。

更に、本発明の請求項 3 に係る発明は、セレクターの出力と物理乱数を入力とする排他的論理和回路を設けその出力を乱数保持装置（200）入力とする請求
5 項 1 に記載の物理乱数の一様化手法である。

また、本発明の請求項 4 に係る発明は、請求項 1 から請求項 3 の何れかの操作を 2 サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法である。

また、本発明の請求項 5 に係る発明は、乱数保持装置としてシフトレジスタ（
10 200）を用いたことを特徴とする請求項 1 から請求項 4 までのいずれかに記載の物理乱数の一様化手法である。

なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

15 次に、本発明のうち請求項 6 に係る発明は、物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成
20 される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えて構成される。ここで、読出しクロックは基準クロックとは別に入力されるものである。

25 また、本発明のうち請求項 7 に係る発明は、前記物理乱数発生器が、複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンタを備え、前記アップ／ダウンカウンタが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード

信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスタのうち後段のレジスタから前段のレジスタへ順次保持し、かつ、読出しクロック信号に応じて前記レジスタのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスタより前段にある各レジスタ内のパラレル乱数
5 数を後段へ順次シフトする制御回路を備えて構成される。

また、本発明のうち請求項 8 に係る発明は、前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンタを備え、前記総数カウンタがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数
10 検証回路を備えて構成される。

また、本発明のうち請求項 9 に係る発明は、前記乱数検証回路の乱数検証方法として、乱数値“0”又は“1”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項 10 に係る発明は、前記乱数検証回路の乱数検証方法として、4 ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出された χ^2 乗値を規定値と比較することによって乱数の一様性を検証する乱数
15 検証方法を採用して構成される。

また、本発明のうち請求項 11 に係る発明は、前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。
20

また、本発明のうち請求項 12 に係る発明は、前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項 13 に係る発明は、チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファ機能をも 3 ステートとして構成される。
25

さらに、本発明のうち請求項 14 に係る発明は、前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにして構成される。

さらに、本発明のうち請求項 15 に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力する増幅器と、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを 2 個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて” 0 ” または” 1 ” を出力するフリップ・フロップを備え、前記各積分回路に入力される入力信号の位相を調整するディレー、第 1 セレクターおよびアップ/ダウンカウンタからなる位相調整部を備え、前記フリップ・フロップから出力される” 0 ” または” 1 ” がそれぞれ 50 % に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、前記各積分回路の前段にそれぞれ第 2 セレクター及び第 3 セレクターを設け、前記アップ/ダウンカウンタの最上位ビットによって前記第 1 セレクターと前記第 2 セレクターおよび前記第 3 セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発生器である。

さらに、本発明のうち請求項 16 に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を 1 個備え、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを 2 個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて” 0 ” または” 1 ” を出力するフリップ・フロップを備えた物理乱数発生器において、前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、前記フリップ・フロップから出力される” 0 ” または” 1 ” がそれぞれ 50 % に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器である。

さらに、上記構成において、前記積分回路の抵抗の後段に FET（電界効果トランジスタ）を当該積分回路のキャパシタと並列に付加した構成とすることでも

きる。

また、上記構成の前記積分回路の抵抗に代えて、定電流回路を設けた構成とすること可能である。

図面の簡単な説明

図 1 A および図 1 B は、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図である。

図 2 A 及び図 2 B は、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図である。

図 3 A 及び図 3 B は、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

図 4 は本発明に係る物理乱数発生装置の第 1 の実施形態を示す回路図。

図 5 は図 4 に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図。

図 6 は図 5 に示す物理乱数発生器の各部の出力波形を示す波形図。

図 7 は図 5 に示す物理乱数発生器の各部の出力波形を示す波形図。

図 8 は図 4 に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回路図。

図 9 は図 4 に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図。

図 10 は図 4 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図。

図 11 は図 4 に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図。

図 12 は図 4 に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

図 13 は本発明に係る物理乱数発生装置の第 2 の実施形態を示す回路図。

図 14 は本発明に係る物理乱数発生装置の第 3 の実施形態を示す回路図。

図 15 は図 14 に示す物理乱数発生装置の各部の出力波形を示す波形図。

図 16 は本発明に係る物理乱数発生器の別の実施形態を示す回路図。

図 1 7 は図 1 6 に示す物理乱数発生器のエッジ検出回路の詳細を示す図。

図 1 8 は図 1 6 に示す物理乱数発生器の動作波形を示す図。

図 1 9 は本発明に係る物理乱数発生器の更に別の実施形態を示す回路図。

図 2 0 は積分回路の別の例を示す回路図。

5 図 2 1 は図 2 0 に示す積分回路を用いた物理乱数発生器の動作波形を示す図。

図 2 2 は積分回路の更に別の例を示す図であり、更に

図 2 3 は、図 2 2 に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。

10 発明を実施するための最良の形態

<発明の第 1 の態様>

以下、本発明の実施形態を図面に基づいて説明する。

まず、図 1 A に示す乱数一様化回路 1 0 0 では、シフトレジスタ 2 0 0 とセレクト
クタ 3 0 0 とを具備しており、シフトレジスタ 2 0 0 のデータ端子 D には 2 進乱
15 数（「0」または「1」）が順次入力され、シフトレジスタ 2 0 0 のクロック端
子 C L K に入力される基準パルス信号が立ち上がるごとに、これらの 2 進乱数が
順に出力 Q 0 0 ~ Q 1 3 4 にシフトされていく。そして、シフトレジスタ 2 0 0
の出力 Q 0 0 ~ Q 1 2 7 の 1 2 8 ビットの乱数はそれぞれセクタ 3 のデータ端
子 D 0 0 ~ D 1 2 7 に入力され、シフトレジスタ 2 0 0 の出力 Q 1 2 8 ~ Q 1 3
20 4 の 7 ビットの乱数はそれぞれセクタ 3 0 0 のアドレス A D 0 ~ A D 6 に入力
される。

その後、セクタ 3 0 0 では、アドレス A D 0 ~ A D 6 に入力された 7 ビット
のアドレス値に応じて、データ端子 D 0 0 ~ D 1 2 7 に入力された 1 2 8 ビット
の乱数から 1 ビットが選択され、出力端子 O U T から出力される。例えば、アド
25 レス A D 0 ~ A D 6 にそれぞれ「1」「0」「0」「0」「0」「0」「0」が
入力されたときは、データ端子 D 0 0 に入力された乱数が出力端子 O U T から出
力される。また、アドレス A D 0 ~ A D 6 にそれぞれ「1」「0」「1」「0」
「0」「0」「0」が入力されたときは、データ端子 D 0 4 に入力された乱数が
出力端子 O U T から出力される。

このように、シフトレジスタ 200 のデータ端子 D に順次入力される 2 進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この 2 進乱数が偏りを持っていても、この乱数一様化回路 1 で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、1 ビットの乱数を出力するのには複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

また、図 1 B に示す乱数一様化回路 100 は、シフトレジスタ 200 からの乱数出力を選択するビット数を 6 ビットに減らしたことで、排他的論理和 (XOR) 回路を追加したことを除き、図 1 A に示す乱数一様化回路 1 と同様である。すなわち、図 1 B に示す乱数一様化回路 1 では、シフトレジスタ 200 とセレクタ 300 とを具備しており、セレクタ 300 の出力と 2 進乱数 (「0」または「1」) とを入力とする排他的論理和回路の出力が順次シフトレジスタ 200 のデータ端子 D に入力され、シフトレジスタ 200 のクロック端子 CLK に入力される基準パルス信号が立ち上がるごとに、出力 Q00 ~ Q69 に順にシフトされていく。そして、シフトレジスタ 200 の出力 Q00 ~ Q63 の 64 ビットの乱数はそれぞれセレクタ 300 のデータ端子 D00 ~ D63 に入力され、シフトレジスタ 2 の出力 Q64 ~ Q69 の 6 ビットの乱数はそれぞれセレクタ 300 のアドレス AD0 ~ AD5 に入力される。その後、セレクタ 300 では、アドレス AD0 ~ AD5 に入力された 6 ビットのアドレス値に応じて、データ端子 D00 ~ D63 に入力された 64 ビットの乱数から 1 ビットが選択され、出力端子 OUT から出力される。

この場合も、シフトレジスタ 200 のデータ端子 D に順次入力される 2 進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この 2 進乱数が偏りを持っていても、この乱数一様化回路 100 で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

このことを確認するため、この乱数一様化回路 100 から出力された乱数の一

様性を乱数検定規格 FIPS 140-2 に準拠して評価した。その結果を表 1 および表 2 に示す。なお、表 1 中の数値は元データを表し、表 2 中の数値は検定結果データを表す。ここで、表 1、2 中の「Mono」、「Poker」、「Runs」および「Long Run」は乱数検定の種類を表しており、それぞれ乱数
5 検定規格 FIPS 140-2 の「Monobit Test」、「Porker Test」、「Runs Test」および「Long Run Test」に対応している。また、結果は 50 回を 1 セットとして表示しており、数値は 50 回の検定中で不合格になった回数を表している。

【表 1】

セット No.	Mono	Poker	Runs	LongRun
1	0	0	1	0
2	0	0	0	0
3	0	0	1	0
4	0	0	1	0
5	0	0	1	0
6	0	0	2	0
7	0	0	0	0
8	0	0	0	0
9	0	0	1	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	1	0
15	0	0	0	0
16	0	0	1	0
17	0	0	1	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	1	1
22	0	0	1	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	1	0
27	0	0	0	0
28	0	0	0	0
29	0	0	1	0
30	1	0	0	0
31	0	0	0	1
32	0	0	1	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	1
36	0	0	1	0
37	0	0	1	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	0	0
42	0	0	0	0
43	0	0	1	0
44	0	0	0	0
45	0	0	0	0
46	0	0	2	0
47	0	0	0	0
48	0	0	1	0
49	0	0	0	0
50	0	0	0	0

【表 2】

セット No.	Mono	Poker	Runs	LongRun
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0
29	0	0	0	0
30	0	0	0	0
31	0	0	0	0
32	0	0	0	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	0
36	0	0	0	0
37	0	0	0	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	1	0
42	0	0	0	0
43	0	0	0	0
44	0	0	0	0
45	0	0	0	0
46	0	0	0	0
47	0	0	0	0
48	1	0	0	0
49	0	0	0	0
50	0	0	0	0

上に示した表 1 及び表 2 から明瞭に理解させるように、4 種類すべての乱数検
定（「Mono」、「Poker」、「Runs」および「Long Run」）
において、セット No. 1 ～ 50 のほとんど全部が合格値となり、上述した効果が確
認された。

5 一方、図 2 A に示す乱数一様化回路 1 は、シフトレジスタ 200 からの乱数出
力を選択するビット数を 15 ビットに増やしたことと、セクタ 300 と同様な
働きをするものとして論理積（AND）回路と排他的論理和（XOR）回路との
組み合わせを代用したことを除き、図 1 A に示す乱数一様化回路 1 と同様である
。すなわち、図 2 A に示す乱数一様化回路 1 ではシフトレジスタ 200 を具備し
10 ており、シフトレジスタ 200 のデータ端子 D には 2 進乱数（「0」または「1
」）が順次入力され、シフトレジスタ 200 のクロック端子 CLK に入力される
基準パルス信号が立ち上がるごとに、これらの 2 進乱数が順に出力 Q00 ～ Q3
0 にシフトされていく。そして、シフトレジスタ 200 の出力 Q00 ～ Q14 の
15 ビットの乱数とシフトレジスタ 200 の出力 Q16 ～ Q30 の 15 ビットの
15 乱数とを入力とする 15 個の論理積回路の出力が、シフトレジスタ 200 の出力
Q15 とともに排他的論理和回路で順次合成されて出力される。

このように、シフトレジスタ 200 のデータ端子 D に順次入力される 2 進乱数
は、シフトレジスタ 200 内で同じビット数（15 ビット）の 2 組に分けられた
後、論理積回路と排他的論理和回路でランダムに演算されるので、この 2 進乱数
20 が偏りを持っていても、この乱数一様化回路 1 で一様化されて出力されることにな
る。しかも、従来のノイマンコレクターと異なり、1 ビットの乱数を出力する
のに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないた
め、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って
、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保するこ
25 とができる。

また、図 2 B に示す乱数一様化回路 100 は、シフトレジスタ 200 からの乱
数出力を選択するビット数を 7 ビットに減らしたことと、排他的論理和（XOR
）回路を追加したことを除き、図 2 A に示す乱数一様化回路 1 と同様である。す
なわち、図 2 B に示す乱数一様化回路 1 ではシフトレジスタ 200 を具備してお

り、シフトレジスタ 200 のデータ端子 D には 2 進乱数（「0」または「1」）が順次入力され、シフトレジスタ 200 のクロック端子 CLK に入力される基準パルス信号が立ち上がるごとに、これらの 2 進乱数が順に出力 Q00～Q14 にシフトされていく。そして、シフトレジスタ 2 の出力 Q00～Q06 の 7 ビット
5 の乱数とシフトレジスタ 2 の出力 Q08～Q14 の 7 ビットの乱数とを入力とする 7 個の論理積回路の出力が、シフトレジスタ 200 の出力 Q07 とともに排他的論理和回路で順次合成され、最後に元の 2 進乱数（生データ）と排他的論理和回路で合成されて出力される。

この場合も、シフトレジスタ 200 のデータ端子 D に順次入力される 2 進乱数
10 は、シフトレジスタ 200 内で同じビット数（7 ビット）の 2 組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この 2 進乱数が偏りを持っていても、この乱数一様化回路 100 で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

なお、上述の実施形態においては、複数の物理乱数を保持する乱数保持装置としてシフトレジスタ 200 を用いた場合について説明したが、シフトレジスタ 2
15 00 以外の乱数保持装置（例えば、フリップフロップ）を代用することも可能である。

また、上述の実施形態においては、1 個の乱数一様化回路 1 を用いて物理乱数を一様化する場合について説明したが、図 3 A 及び図 3 B に示すように、図 1 A
20 、図 1 B や図 2 A、図 2 B に示す乱数一様化回路 100 （CKT1, CKR2, … CKTx）を 2 個以上接続して物理乱数を多段に一様化することもできる。この場合、乱数一様化回路 100 の接続方法は、図 3 A に示すような直列接続であっても、図 3 B に示すような並列接続であっても構わない。

以上説明したように、本発明によれば、乱数保持装置（シフトレジスタ）に入
25 力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られてしまう事態が起きないことから、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することができる。

＜発明の第２の態様＞

次に、本発明の物理乱数発生器の好適な実施例について図面の図４～図１５を参照して説明する。

この物理乱数発生装置９１は、図４に示すように、物理乱数発生器１、乱数検証回路２１、制御回路９４、カウンタ９５、第１セレクタ９６、第２セレクタ９７から構成されており、物理乱数発生器１は、図５に示すように、シリアル物理乱数発生器２、カウンタ３、シフトレジスタ４、複数個（図５ではｍ個）のレジスタ５、制御回路６、アップ／ダウンカウンタ７、セレクタ８、基準クロック側の２個の遅延回路９および読出しクロック側の２個の遅延回路１０から構成されている。

他方、乱数検証回路２１は、図８から図１２までに示すように、乱数検定規格ＦＩＰＳ１４０－２に準拠した４種類の検定方法（MonobitTest、PokerTest、RunsTestおよびLongRunsTest）に対応する部分から構成されている。すなわち、MonobitTestに関する部分は、図８に示すように、第１カウンタ２３、第２カウンタ２４、レジスタ２５、制御回路２６および比較器２７から構成されており、PokerTestに関する部分は、図９に示すように、第１カウンタ３３、シフトレジスタ３４、デコーダ３５、複数個（図９では１６個）のカウンタ３６、制御回路３７、セレクタ３８、掛算器３９、加算器４０、レジスタ４１および比較器４２から構成されている。また、RunsTestに関する部分はさらに乱数出力が“１”の場合と乱数出力が“０”の場合とに二分され、前者は、図１０に示すように、第１カウンタ５３、比較器５４、データ保持器５５、第２カウンタ５６、制御回路５７、デコーダ５８、６個のカウンタ５９および６個の比較器６０から構成されており、後者は、図１１に示すように、物理乱数発生器１のシリアル物理乱数発生器２からデコーダ５８への出力線上にインバータが設けられて出力が反転する点を除き、前者と同じ構成を有している。さらに、LongRunsTestに関する部分は、図１２に示すように、第１カウンタ７３、比較器７４、データ保持器７５、制御回路７６、第２カウンタ７７、第１比較器７８、レジスタ７９および第２比較器８０から構成されている。

物理乱数発生装置９１は以上のような構成を有するので、この物理乱数発生装

置 9 1 を作動させると、まず物理乱数発生器 1 で、シリアル乱数が出力されるとともに、パラレル乱数が保持されて必要に応じて出力できる状態となる。

すなわち、基準クロック (CLK_0) でシリアル物理乱数発生器 2 より生成されたシリアル乱数 (SRND) をカウンタ 3 のキャリアウト (C0) に同期して、シフトレジスタ 4 でシリアルからパラレルに変換した n ビットの乱数 (CRND) をセレクタ 5
5 セレクタ 8 で選択されたレジスタ 5 にロードしてパラレル乱数を保持する。

このとき、セレクタ 8 はアップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) で指定されたレジスタ 5 を選択し、カウンタ 3 のキャリアウト (C0) に同期してパラレル乱数 (CRND) をレジスタ 5 にロードし、ロードごとに
10 アップ/ダウンカウンタ 7 をカウントアップし、アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) が m になった時点で、アップ/ダウンカウンタ 7 はカウントアップとパラレル乱数のロードを中止し、以降その状態を維持する。

パラレル乱数の出力 (PRND) は最下位のレジスタ 5 の出力とし、読み出し後に
15 読出しクロック (CLK_R) を入力し、読出しクロックにてアップ/ダウンカウンタ 7 のカウントダウンとすべてのレジスタ 5 内のデータを上位から下位へシフトし、パラレル乱数 (PRND) はその都度更新される。アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) がゼロになった時点で、アップ/ダウンカウンタ 7 はカウントダウンとデータシフトを中止し、以降その状態を維持する。

20 アップ/ダウンカウンタ 7 の出力の書込みアドレス (ADDRESS) は外部に出力され、すべてのレジスタ 5 に保持されているパラレル乱数の数を逐次モニター可能とする。

遅延回路 9、10 は各クロックのエッジ (例えば、立上りエッジ) を取り出し、非常に短いパルス波形 (例えば、10 ns) を生成し、アップ/ダウンカウンタ 7 とすべてのレジスタ 5 のクロック信号 (CLOCK)、アップ/ダウンカウンタ 7 の ENABLE 信号、すべてのレジスタ 5 の SHIFT 信号と LOAD(0) ~ LOAD($m-1$)
25 を生成する。これにより、基準クロック (CLK_0) と読出しクロック (CLK_R) が非同期または同期式で動作するとき、基準クロック (CLK_0) のエッジ (例えば、立上りエッジ) に対する読出しクロック (CLK_R) のエッジ (例えば、立上りエッジ

）の禁止域($td_Ra + td_0a + 2 \times td_mg$)を非常に小さくして基準クロック(CLK_0)と読出しクロック(CLK_R)との干渉を最小限とすることができる。なお、CLK_0bとCLK_Rbがクロック信号(CLOCK)を生成し、CLK_0aとCLK_RaがENABLE信号、SHIFT信号とLOAD(0)～LOAD(m-1)を生成する。

5 制御回路6はカウンタ3のキャリーアウト(CO)の同期信号(SYNC)、CLK_0a、CLK_Ra、アップ/ダウンカウンタ7のOVER信号とZERO信号より、アップ/ダウンカウンタ7のUP/DOWN信号とENABLE信号、すべてのレジスタ5のSHIFT信号とLOAD(0)～LOAD(m-1)用のLOAD信号を生成する。

こうすることにより、基準クロックに同期してシリアル物理乱数発生器2で生成されたシリアル乱数よりn倍の周期で最大m個のnビットの平行乱数を保持することができる。それ以降のシリアル乱数は読み出し操作(CLK_Rの入力)をするまでは保持されない。こうして保持された最大m個の平行乱数は読出しクロックで必要なときに必要な量(最大m個)を短時間に集中して読み出すことができ、読み出された量の平行乱数は逐次補充される。基準クロック(CLK_0)のエッジに対する読出しクロックのエッジの禁止域が非常に狭く、非同期または同期式でタイミングよく、かつ効率的に読み出すことができる。書込みアドレスを読み出すことで、その時点で保持された平行乱数の量を確認することが可能となり、乱数を効率的に活用することができる。

ところで、こうしてシリアル物理乱数発生器2で生成されたシリアル乱数は、
20 乱数検定規格FIPS140-2に準拠した4種類の検定方法(MonobitTest、PokerTest、RunsTestおよびLongRunsTest)でその一様性が検証される。

まず、MonobitTestによる検証が行われる。すなわち、図8に示すように、第1カウンタ23はスタート信号(START)と基準クロック(CLK_0)より制御回路26を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。第2カウンタ24は制御回路26の出力信号CLR_C2でスタート信号(START)が入った時点で初期化を行い、シリアル乱数(SRND)の“1”または“0”をカウントする。レジスタ25は制御回路26の出力信号LOAD_Rでスタート信号(START)が入った時点より20,000クロック時の第2カウンタ24のカウント値をロードして保持し、MonobitData(MOND)を出力する。比較器2

7はレジスタ25の出力MonobitData(MOND)と上限比較データ(例えば、10,275bit)および下限比較データ(例えば、9,725bit)とを比較し、MonobitJudge(MONJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にMonobitDataとMonobitJudgeを検証することができる。

次に、PokerTestによる検証が行われる。すなわち、図9に示すように、第1カウンタ33はスタート信号(START)と基準クロック(CLK_0)より制御回路37を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。シフトレジスタ34はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次4ビットの平行乱数(PRND_4B)に変換する。デコーダ35は、スタート信号(START)と基準クロック(CLK_0)より制御回路37を介して生成されたENABLE信号がアクティブのとき(4クロックごとに1回)に平行乱数(PRND_4B)で指定された出力部(SE_0~SE_15)に出力される。カウンタ36は制御回路37の出力信号CLR_CRでスタート信号(START)が入った時点に初期化を行い、ENABLE信号がアクティブのとき(4クロックごとに1回)に平行乱数(PRND_4B)のデータにてデコーダ35で指定されたカウンタ36をカウントアップする。すべてのカウンタ36の総計は5,000カウントとなり、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にその間の4ビットごとの平行乱数(PRND_4B)のデータ(0~15)の度数分布データ(PokerData0~PokerData15)を取得する。レジスタ41は、制御回路37の出力信号CLR_CRでスタート信号(START)が入った時点に初期化(POKD=0)を行い、度数分布データ(PokerData0~PokerData15)を取得した後、セレクタ38、掛算器39、加算器40を介して度数分布データ(PokerData0~PokerData15)の16個の二乗和を求めることでPokerData(POKD)を取得する。比較器42はレジスタ41の出力PokerData(POKD)と上限比較データ(例えば、1,576,928)および下限比較データ(例えば、1,563,175)とを比較し、PokerJudge(POKJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000+16クロック後にPokerDataとPokerJudgeを検証することができる。

次いで、RunsTestによる検証が行われる。すなわち、図10および図11に示すように、第1カウンタ53はスタート信号(START)と基準クロック(CLK_0)より制御回路57を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器55はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次1ビット保持し、比較器54はシリアル乱数(SRND)とデータ保持器55で保持された乱数を比較し、1クロック前の乱数と今回の乱数が変化したときに信号CHANGEを出力する。第2カウンタ56は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号RUNS_Dを出力する。信号RUNS_Dと同一信号の長さ(L)の関係は $L = \text{RUNS_D} + 1$ となる。第2カウンタ56は、制御回路57の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化($\text{RUNS_D} = 0$)を行う。デコーダ58は、スタート信号(START)、基準クロック(CLK_0)、第1カウンタ53の出力(OUT_C)と比較器54の出力(CHANGE)より制御回路57を介して生成されたENABLE信号がアクティブ(CHANGEがアクティブ)のときで、図10ではシリアル乱数(SRND)が“1”のとき、図11ではシリアル乱数(SRND)が“0”のとき、第2カウンタ56の出力(RUNS_D)で選択された出力(SE_1~SE_6+)をアクティブにする。なお、 $L=1 \rightarrow \text{SE}_1$ 、 $L=2 \rightarrow \text{SE}_2$ 、…、 $L=6+ \rightarrow \text{SE}_6+$ となる。すべてのカウンタ59は、制御回路57の出力信号CLR_Cでスタート信号(START)が入った時点に初期化を行い、デコーダ58の出力(SE_1~SE_6+)で指定されたカウンタ59をカウントアップし、1~6+の同一信号の長さ(L)の出現回数(図10ではRunsData1H~RunsData6+H、図11ではRunsData1L~RunsData6+L)を取得する。各比較器60は各カウンタ59の出力(図10ではRunsData1H~RunsData6+H、図11ではRunsData1L~RunsData6+L)とそれぞれの上限比較データ(例えば、2,685、1,386、723、384、209、209)および下限比較データ(例えば、2,315、1,114、527、240、103、103)とを比較し、判定信号(図10ではRunsJudge1H~RunsJudge6+H、図11ではRunsJudge1L~RunsJudge6+L)を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にRunsTestのデータと判定を検証することができる。

最後に、LongRunsTestによる検証が行われる。すなわち、図12に示すように

、第1カウンタ73はスタート信号(START)と基準クロック(CLK_0)より制御回路57を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器75はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次1ビット保持し、比較器74はシリアル乱数(SRND)とデータ保持器75で保持された乱数を比較し、1クロック前の乱数と今回の乱数に変化したときに信号CHANGEを出力する。第2カウンタ77は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号LRUNS_Dを出力する。

第2カウンタ77は、制御回路76の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(LRUNS_D=0)を行う。レジスタ79は、制御回路76の出力信号CLR_Rでスタート信号(START)が入ったときに初期化(LRUNS_D=0)を行う。レジスタ79の出力信号LongRunsData(LRND)と第2カウンタ77の出力信号(LRUNS_D)を第1比較器78で比較し、LRND<LRUNS_Dのときに第1比較器78は出力信号COMP_Uを出力し、制御回路76を介してレジスタ79にLOAD_R信号を出力して、レジスタ79に逐次LRUNS_Dの最大値を保持する。第2比較器80は上限比較データ(例えば、26)と比較し、判定信号LongRunsJudge(LRNJ)を出力する。信号LRUNS_D、LRNDと同一信号の長さ(L)の関係は $L=LRUNS_D+1$ 、 $L(\max)=LRND+1=LRUNS_D(\max)+1$ となる。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にLongRunsTestのデータと判定を検証することができる。

そして、こうして4種類の検定方法で検証された一様性乱数の検証データは、図4に示すように、第2セレクタ97に保持され、使用者の要望に応じて出力される。選択信号(A0、A1)と動作テーブルを表3に示す。

【表3】

ADDRE_S	A1	A0	読出しクロック(CLK_R)の働き	出力(DATA BUS)
0	0	0	パラレル物理乱数の更新	パラレル物理乱数
1	0	1	パラレル物理乱数の更新	パラレル物理乱数の生成状態
2	1	0	乱数検証のスタート／カウンタの初期化	乱数検証状態／モニターアドレス
3	1	1	乱数検証のモニターアドレス更新	乱数検証結果／検証データ

25

すなわち、物理乱数発生器1は、選択信号(A1)の状態(“0”または“1”)

により、読出しクロック (CLK_R) でのパラレル乱数の更新 (アップ/ダウンカウンタ 7 のカウントダウン) または非更新とする。出力のパラレル乱数 (PRND) は第 2 セレクター 9 7 の DATA_0 に接続される。出力 (COND_R) には書込みアドレス (ADDRESS) などの物理乱数生成時およびパラレル乱数変換時に生成される各種データやフラグを出力し、第 2 セレクター 9 7 の DATA_1 に接続される。

乱数検証回路 2 1 は、選択信号 (A0、A1) が 2 (ADDRE_S) のときに制御回路 9 4 を介して読出しクロック (CLK_R) 信号で検証を開始し、MonobitTest、PokerTest、RunsTest および LongRunsTest を基準クロック (CLK_0) で 20,000+16 サイクルで完了し、判定結果、判定データ、PokerTest の生データを出力して第 1 セレクター 9 6 に接続される。その詳細を表 4 に示す。

【表 4】

モニターアドレス (SEL_ADD)	出力 (DATA BUS)
0	0 ; Monobit Judge (MONJ) 1 ; Poker Judge (POKJ) 2 ; Runs Judge 1H (RUNJ1H) 3 ; Runs Judge 1L (RUNJ1L) 4 ; Runs Judge 2H (RUNJ2H) 5 ; Runs Judge 2L (RUNJ2L) 6 ; Runs Judge 3H (RUNJ3H) 7 ; Runs Judge 3L (RUNJ3L) 8 ; Runs Judge 4H (RUNJ4H) 9 ; Runs Judge 4L (RUNJ4L) 10 ; Runs Judge 5H (RUNJ5H) 11 ; Runs Judge 5L (RUNJ5L) 12 ; Runs Judge 6+H (RUNJ6+H) 13 ; Runs Judge 6+L (RUNJ6+L) 14 ; Long Run Judge (LRNJ) 15 ; 総合判定
1	Monobit Data (MOND)
2	Poker Data (POKD)
3	Runs Data 1H (RUND1H)
4	Runs Data 1L (RUND1L)
5	Runs Data 2H (RUND2H)
6	Runs Data 2L (RUND2L)
7	Runs Data 3H (RUND3H)
8	Runs Data 3L (RUND3L)
9	Runs Data 4H (RUND4H)
10	Runs Data 4L (RUND4L)
11	Runs Data 5H (RUND5H)
12	Runs Data 5L (RUND5L)
13	Runs Data 6+H (RUND6+H)
14	Runs Data 6+L (RUND6+L)
15	Long Run Data (LRND)
16	Poker Data 0 (POK_0)
17	Poker Data 1 (POK_1)
18	Poker Data 2 (POK_2)
19	Poker Data 3 (POK_3)
20	Poker Data 4 (POK_4)
21	Poker Data 5 (POK_5)
22	Poker Data 6 (POK_6)
23	Poker Data 7 (POK_7)
24	Poker Data 8 (POK_8)
25	Poker Data 9 (POK_9)
26	Poker Data 10 (POK_10)
27	Poker Data 11 (POK_11)
28	Poker Data 12 (POK_12)
29	Poker Data 13 (POK_13)
30	Poker Data 14 (POK_14)
31	Poker Data 15 (POK_15)

なお、総合判定はすべての判定結果が合格のときに出力される。出力(COND_T)には、乱数検証時に生成される各種データやフラグを出力し、第2セレクター97のDATA_2にカウンタ出力のモニターアドレス(SEL_ADD)とともに接続される。また、検証のスタート信号にてパラレル乱数生成用のカウンタ3、シフトレジスタ4、アップ/ダウンカウンタ7とすべてのレジスタ5は初期化され、検証された物理乱数を保持して検証後の物理乱数を使用することができる。

カウンタ95は第1セレクター96のモニターアドレス(SEL_ADD)を生成する。カウンタ95は、制御回路94の出力信号(CLR_C)で選択信号(A0、A1)が2(ADDRE_S)のときに読出しクロック(CLK_R)信号で検証を開始し、この開始時に初期化を行い、制御回路94の出力信号(CLR_C)で選択信号(A0、A1)が3(ADDRE_S)のときに読出しクロック(CLK_R)信号でカウンタ95のカウントアップ(更新)を行う。

これにより、基準クロックに同期して生成されたシリアル乱数(SRND)と逐次補充されるパラレル乱数(PRND)の生成及び一様性の検証を逐次行うことができる。

こうすることにより、物理乱数発生器1の検証およびデータの確認が容易となり、検証後の乱数を活用することができる。選択信号(A0、A1)と第2セレクター97を用いることで入出力端子を大幅に減らすことができる。選択信号(A0、A1)、読出しクロック(CLK_R)、カウンタ95と第2セレクター97で、参照できる有効な検証データを拡大することができる。

なお、図13に示すように、物理乱数発生器1にチップセレクト(CS)と出力イネーブル(OE)の入力を付加し、パラレル乱数[PRND(0)~PRND(n-1)]の出力形態を3ステート(“0”、“1”、off)にすることもできる。

また、図14および図15に示すように、複数個(図14ではp個)の物理乱数発生器1とセレクター12とで高速(図14ではp倍)の乱数生成スピードを獲得することも可能である。ここで、基準クロック(CLK_0)のエッジ(例えば、立上りエッジ)に対する読出しクロック(CLK_R)のエッジ(例えば、立上りエッジ)の禁止域($td_{Ra} + td_{0a} + 2 \times td_{mg}$)を非常に狭く考慮することのみで非同期または同期式の高速乱数発生を容易に実現することができる。

このように、チップセレクト(CS)と出力イネーブル(OE)を有することで、物理

乱数発生器 1 を複数個接続することが容易となり、乱数生成の高速化が可能となる。また、チップセレクト (CS) と出力イネーブル (OE) を有することで、CPU を使用したシステムに物理乱数発生器 1 を容易に接続することができる。

なお、上述の実施形態では、基準クロック (CLK_0) のエッジに対する読出しクロック (CLK_R) のエッジの禁止域 ($td_Ra + td_0a + 2 \times td_mg$) を非常に小さくして基準クロック (CLK_0) と読出しクロック (CLK_R) との干渉を最小限とするため、基準クロック側および読出しクロック側にそれぞれ 2 個の遅延回路 9、10 を設けた場合について説明したが、基準クロック側と読出しクロック側のいずれか一方にだけ遅延回路 9、10 を設けてもよく、遅延回路 9、10 の個数も 1 個以上であれば何個でも構わない。或いはまた、遅延回路 9、10 に代えて波形成形回路（例えば、単安定マルチバイブレータ）を付加しても、同じ効果を得ることができる。

以上説明したように、本発明の上記第 2 の態様のうち請求項 4 ～ 10 に係る発明によれば、生成された物理乱数を効率よく利用することができるとともに、その乱数の一様性を容易に検定して使用することができ、かつ、簡単な回路構成によりこれらを実現することが可能となる。

また、本発明の第 2 の態様のうち請求項 11 および 12 に係る発明によれば、複数個の物理乱数発生 IC を用いて高速に乱数を発生させることが容易となり、かつ、Data Bus に直接接続できるようになるため、物理乱数発生装置の使い易さが格段に向上する。

<発明の第 3 の態様>

本発明の更に別の実施態様において、図 16 および図 18 に示すように、抵抗 R およびキャパシタ（コンデンサ）C でクロック信号を積分して積分波形を出力する積分回路 105 と、ノイズ源 106 と、このノイズ源 106 のノイズを増幅してノイズ信号を出力する増幅器 107 と、積分波形とノイズ信号とをミキシングするミキサー 108 と、このミキサー 108 の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路 109 とが 2 個ずつ設けられている。各エッジ検出回路 109 は、図 17 に示すような回路構成となっており、これらのエッジ検出回路 109 の後段には、図 16 に示すように、各エッジ検

出回路 109 の出力信号の位相差に基づいて” 0 ” または ” 1 ” を出力する D タイプのフリップ・フロップ 110 が設けられている。更に、フリップ・フロップ 110 の後段には、乱数をクロック信号に同期させる D タイプのフリップ・フロップ 111 が設けられている。

5 また、物理乱数発生器 101 の最前段には、各積分回路 105 に入力される入力信号の位相を調整する位相調整部 102 が設けられており、この位相調整部 102 はディレー 121、第 1 セレクター 122 及びアップ／ダウンカウンタ 123 から構成されている。

また、フリップ・フロップ 111 の出力とアップ／ダウンカウンタ 123 と
10 の間にはフィードバック回路 103 が設けられており、フリップ・フロップ 111 ~ 出力される ” 0 ” または ” 1 ” がそれぞれ 50 % に収束するようにフリップ・フロップ 111 の出力が位相調整部 102 にフィードバックされる。すなわち、フィードバック回路 103 は第 1 カウンタ 131、比較器 132、第 2 カウンタ 133、レジスタ 134、比較器 135、シフトレジスタ／レジスタ
15 ー 136、加算機 137 から構成されており、第 1 カウンタ 131 および比較器 132 はフィードバックの周期を乱数 ($2 \times m$) で生成する。また、第 2 カウンタ 133、レジスタ 134 および比較器 135 はフィードバックの周期 ($2 \times m$) 中の ” 0 ” または ” 1 ” の数をカウント (n) し、比較データをアップ／ダウンカウンタ 123 に出力して乱数の一様性を補正するフィードバック信号
20 を出力する。さらに、シフトレジスタ／レジスタ 136 および加算機 137 は、フィードバックの周期を決める乱数 (m) を出力 (OUT) より取得する。これにより、フィードバック周期による乱数の質の低下 (癖) を防ぐことができる。

さらに、位相調整部 102 各積分回路 105 との間にはそれぞれ第 2 セレクター
25 ー 115 および第 3 セレクター 116 が設けられていると共に、第 1 セレクター 122 とアップ／ダウンカウンタ 123 との間には極性切換回路 113 が設けられており、表 5 に示すように、アップ／ダウンカウンタ 123 の最上位ビット MSB によって第 1 セレクター 122 と第 2 セレクター 115 および第 3 セレクター 116 との入力の極性切換が行われる。

【表 5】

アップ/ダウンカウンタ	SELECT	第1セレクターのアドレス	第2セレクターの出力	第3セレクターの出力	相対的な時間差
1Fh 1Eh ⋮ 02h 01h 00h	1 ⋮ 1 ⋮ 1 ⋮ 1	1Fh 1Eh ⋮ 02h 01h 00h	0(A) 0(A) ⋮ 0(A) 0(A) 0(A)	P-1(A) P-2(A) ⋮ 2(A) 1(A) 0(A)	P P-1 ⋮ 3 2 1
3Fh 3Eh ⋮ 22h 21h 20h	0 ⋮ 0 ⋮ 0 ⋮ 0	00h 01h 02h ⋮ 1Eh 1Fh	0(B) 1(B) 2(B) ⋮ P-2(B) P-1(B)	-1(B) -1(B) -1(B) ⋮ -1(B) -1(B)	0 -1 -2 ⋮ -P+2 -P+1

したがって、2系統の信号ラインに応じた2個のディレーおよびセレクターを必要とする従来の物理乱数発生器と比べて、ディレー121及び第1セレクター122を半分にしてゲート数を削減することができるので、物理乱数発生器101の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

図19は本発明の更に別の実施例による物理乱数発生器の回路図である。この物理乱数発生器101においては、図19に示すように、抵抗RおよびキャパシタCでクロック信号を積分して積分波形を出力する積分回路104が1つ設けられており、ノイズ源106と、このノイズ源106のノイズを増幅してノイズ信号を出力する増幅器107と、積分波形とノイズ信号とをミキシングするミキサー108と、このミキサー108の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路109とが2個ずつ設けられている。これらのエッジ検出回路109の後段には、各エッジ検出回路9の出力信号の

位相差に基づいて” 0 ” または” 1 ” を出力する D タイプのフリップ・フロップ 1 1 0 が設けられており、フリップ・フロップ 1 1 0 の後段には、乱数をクロック信号に同期させる D タイプのフリップ・フロップ 1 1 0 が設けられている。

また、フリップ・フロップ 1 1 0 と各エッジ検出回路 1 0 9 との間（各エッジ
5 検出回路 1 0 9 の後段）にはそれぞれ、ディレーとセレクトーからなる可変ディレー 1 1 9 が設けられており、フリップ・フロップ 1 1 0 に入力される入力信号の位相を調整することができる。

さらに、フリップ・フロップ 1 1 1 の出力とアップ／ダウンカウンタ 1 2 3 との間にはフィードバック回路 1 0 3 が設けられており、フリップ・フロップ
10 1 1 から出力される” 0 ” または” 1 ” がそれぞれ 5 0 % に収束するようにフリップ・フロップ 1 1 1 の出力が可変ディレー 1 1 9 にフィードバックされる。

したがって、2 系統の信号ラインについて積分回路 1 0 5 が 1 つで済むことに加えて、積分回路 1 0 5 を構成する抵抗 R、キャパシタ C の誤差による位相調整
範囲を狭めることができるため、ディレーとセレクトーからなる可変ディレー 1
15 1 9 を縮小し、ゲート数を削減することができることから、物理乱数発生器 1 0 1 の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

尚、上記の第 1 9 図に示した実施形態において、図 2 0 に示すように、積分回路 1 0 5 の抵抗 R の後段に F E T （電界トランジスタ） 1 1 7 をキャパシタ C と
20 並列に付加してもよい。この場合は、図 2 1 に示すように、積分回路 1 0 5 のキャパシタ C に充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点が常に安定し、その結果としてジッターの分布も安定する。さらに、ジッターの分布が安定することは良質な乱数を生成することにつながる。
また、乱数生成は電位が基点に戻るまで待たなければならないが、積分回路 1 0
25 5 のキャパシタ C に充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間を短縮することができる。それに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げる
ことができるので、さらなる時間短縮が可能となる（乱数生成したら、すぐに電位を基点まで戻せる）。これにより、乱数生成スピードを大幅に高速化す

ることができる。同様に、上述した図 1 6 ～ 図 1 8 に示した実施形態において、各積分回路 1 0 5 の抵抗 R の後段に F E T 1 1 7 をキャパシタ C と並列に付加することもできる。

また、上記図 1 9 に示した実施形態において、図 2 2 に示すように、積分回路 1 0 5 の抵抗 R に代えて、定電流回路 1 1 8 も設けても構わない。この場合は、図 2 3 に示すように、キャパシタ C の充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みがなくなるため、乱数の質が向上する。同様に、上述した図 1 6 ～ 図 1 8 の実施形態において、各積分回路 1 0 5 の抵抗 R に代えて定電流回路 1 1 8 を設けることも可能である。

また、図 3 B の実施例について説明したと同様に、上述した物理乱数発生器 1 0 1 を k 個（k は 2 以上の数値）並列に接続し、各物理乱数発生器 1 0 1 に入力されたパラレル物理乱数を k 個のシリアル物理乱数に並べ替え、排他的論理和（X O R）素子を介して出力することにより、複数個の物理乱数発生器 1 0 1 からなる物理乱数発生装置の乱数の質を向上させることができる。

また、図 1 6 ～ 図 1 8 の実施形態及び図 1 9 の実施形態においては、乱数発生用のフリップ・フロップとして D タイプのフリップ・フロップを用いた場合について説明したが、本発明ではこれに限定されるわけではなく、これと同等の機能を有するフリップ・フロップであれば代用できる。

また、図 1 9 の実施形態においては、図示の如く、ディレーとセレクターからなる可変ディレー 1 1 9 をエッジ検出回路 1 0 9 の後段に設けた場合について説明したが、可変ディレー 1 1 9 をエッジ検出回路 1 0 9 の前段に設けてもよい。

請 求 の 範 囲

1. 複数の物理乱数を乱数保持装置（２００）に入力して保持し、この乱数保持装置に保持された物理乱数の一部をセレクターのアドレスとして使用し、そのアドレスに基づいて残りの部分から乱数をランダムに選択して出力することを特徴とする物理乱数の一様化手法。
2. 前記セレクターに代え、論理積回路を用い乱数保持装置に保持された乱数をランダムに選択して、それらの排他的論理和を出力することを特徴とする物理乱数の一様化手法。
3. セレクターの出力と物理乱数を入力とする排他的論理和回路を設けその出力を乱数保持装置（２００）入力とする請求項１に記載の物理乱数の一様化手法。
4. 請求項１から請求項３の何れかの操作を２サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法。
5. 乱数保持装置としてシフトレジスタ（２００）を用いたことを特徴とする請求項１から請求項４までのいずれかに記載の物理乱数の一様化手法。
6. 物理乱数発生器を有する物理乱数発生装置であって、該物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えたことを特徴とする物理乱数発生装置。

7. 前記物理乱数発生器が、

複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ/ダウンカウンタを備え、

- 5 前記アップ/ダウンカウンタが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、

前記セレクターからのロード信号に基づいて前記シリアル/パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスター
10 へ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたことを特徴とする請求項4に記載の物理乱数発生装置。

15 8. 前記物理乱数発生器が、

前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンタを備え、

- 前記総数カウンタがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路
20 を備えたことを特徴とする請求項6または請求項7に記載の物理乱数発生装置。

9. 前記乱数検証回路の乱数検証方法として、

- 乱数値“0”または“1”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする
25 請求項8に記載の物理乱数発生装置。

10. 前記乱数検証回路の乱数検証方法として、

4ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出された χ^2 乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法

を採用したことを特徴とする請求 8 に記載の物理乱数発生装置。

1 1. 前記乱数検証回路の乱数検証方法として、

連の長さ別にその出現度数をカウントし、これらを規定値と比較することによ
5 って乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 8
に記載の物理乱数発生装置。

1 2. 前記乱数検証回路の乱数検証方法として、

所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによ
10 って乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項 8
に記載の物理乱数発生装置。

1 3. チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力
部のバッファ機能を 3 ステートとしたことを特徴とする請求項 6 から請求項 1
15 2 までのいずれかに記載の物理乱数発生装置。

1 4. 前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき
、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力
するようにしたことを特徴とする請求項 6 から請求項 1 3 までのいずれかに記載
20 の物理乱数発生装置。

1 5. 抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分
回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力する増
幅器と、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミ
25 キサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッ
ジ検出回路とを 2 個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて” 0 ”または” 1 ”を出
力するフリップ・フロップを備え、

前記各積分回路に入力される入力信号の位相を調整するディレー、第 1 セレク

ターおよびアップ/ダウンカウンタからなる位相調整部を備え、

前記フリップ・フロップから出力される”0”または”1”がそれぞれ50%に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、

- 5 前記各積分回路の前段にそれぞれ第2セレクター及び第3セレクターを設け、
前記アップ/ダウンカウンタの最上位ビットによって前記第1セレクターと前記第2セレクターおよび前記第3セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発生器。

- 10 16. 抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を1個備え、

ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出

- 15 回路とを2個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて”0”または”1”を出力するフリップ・フロップを備えた物理乱数発生器において、

前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け

20 、

前記フリップ・フロップから出力される”0”または”1”がそれぞれ50%に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器。

- 25 17. 前記積分回路の抵抗の後段にFET（電界効果トランジスタ）を当該積分回路のキャパシタと並列に付加したことを特徴とする請求項15又は請求項16の物理乱数発生器。

18. 前記積分回路の抵抗に代えて、定電流回路を設けたことを特徴とする請求

項 1 5 から請求項 1 7 までのいずれかに記載の物理乱数発生器。

1 9. 請求項 1 5 から請求項 1 8 までのいずれかに記載の物理乱数発生器を 2 個
以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリア
5 ル物理乱数に並べ替えて出力するようにした物理乱数発生装置。

FIG. 1A

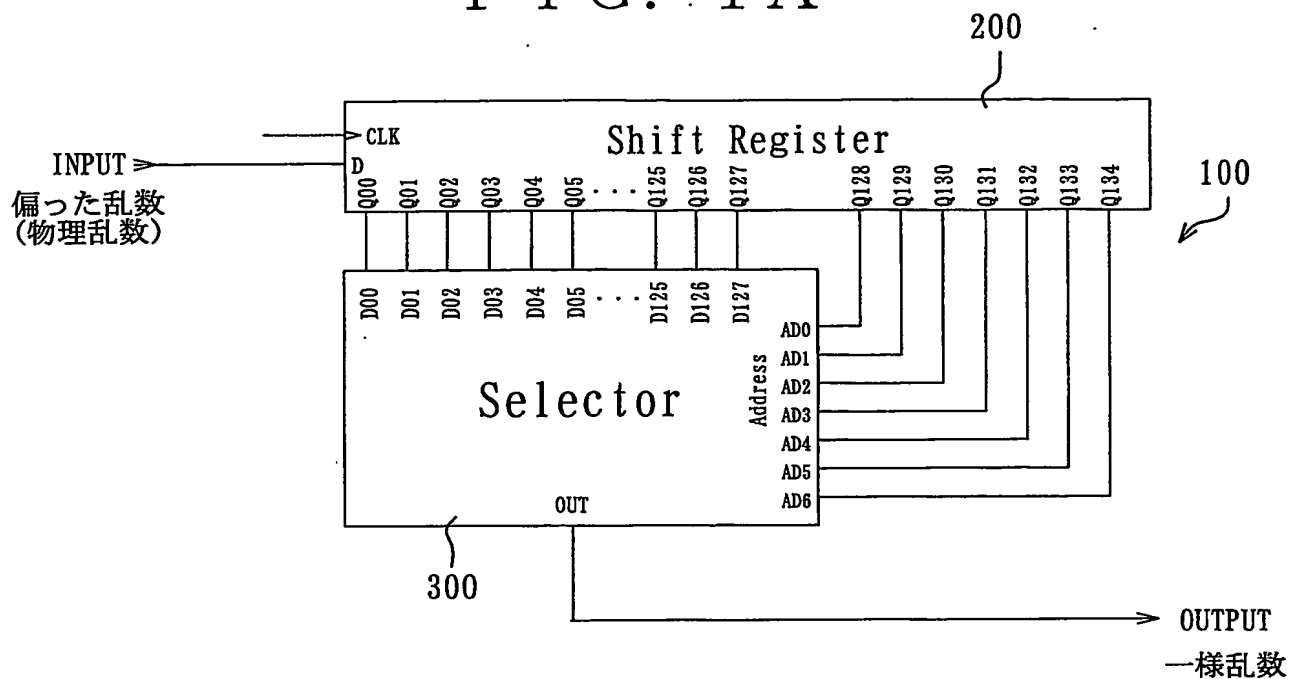


FIG. 1B

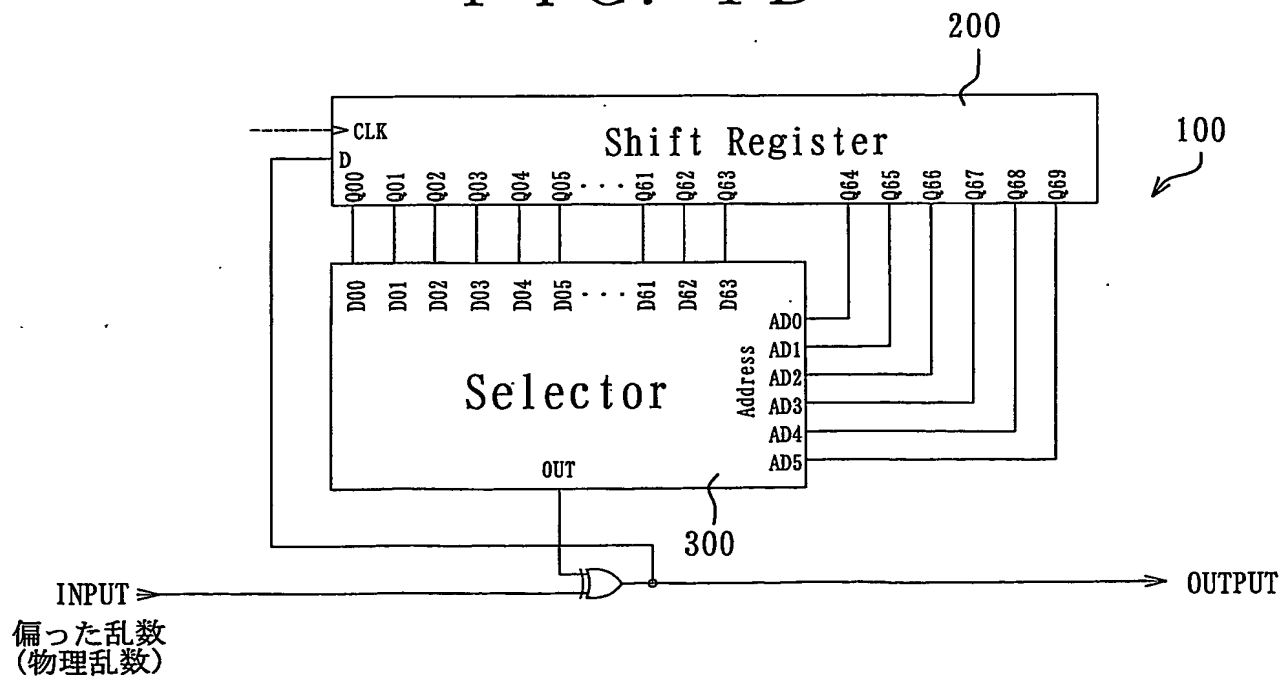


FIG. 2A

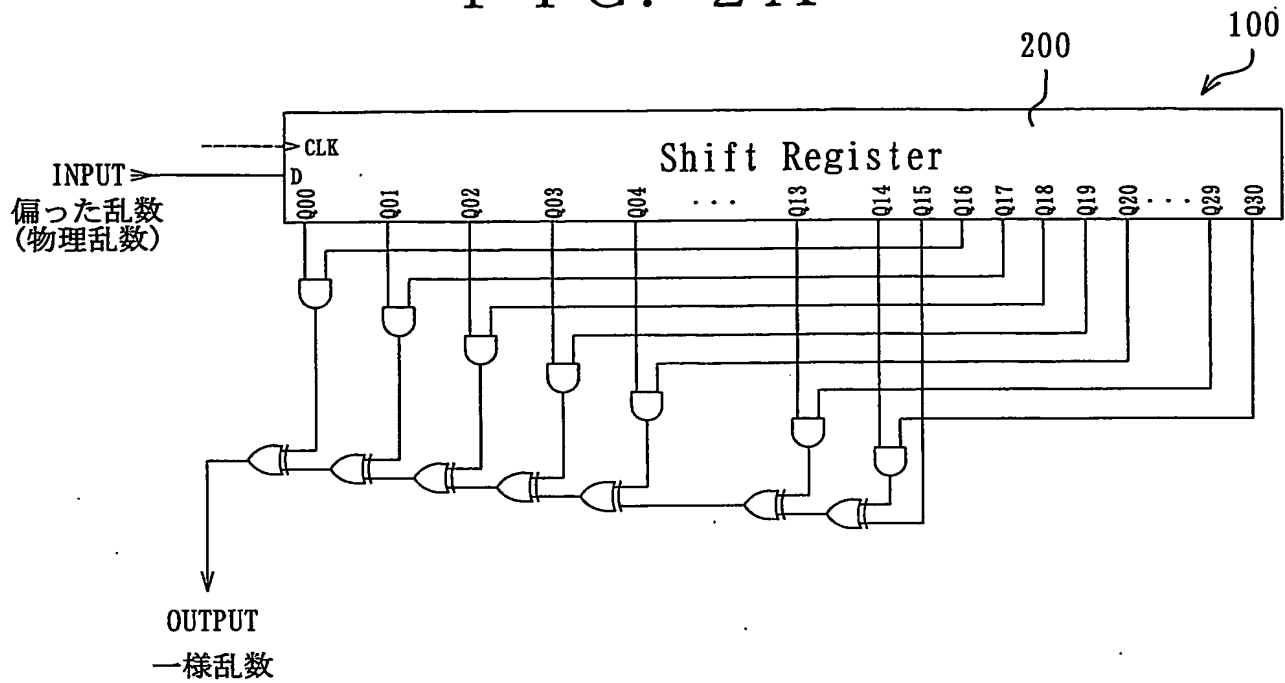


FIG. 2B

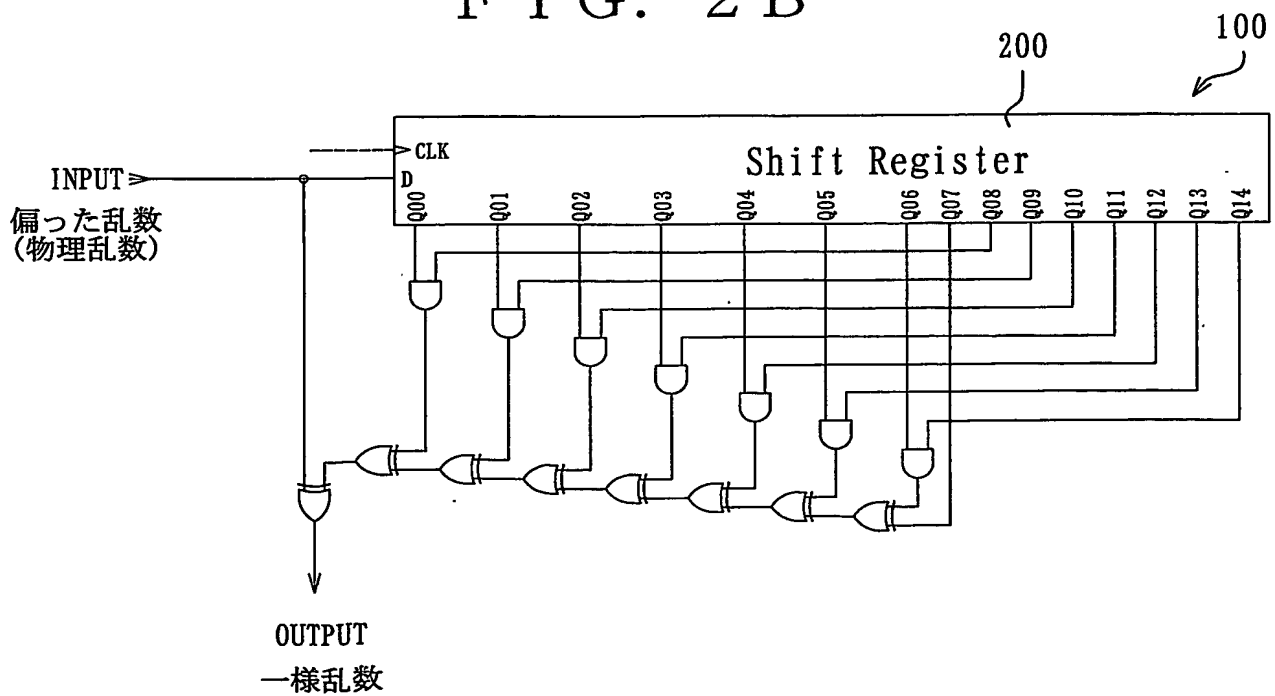


FIG. 3A

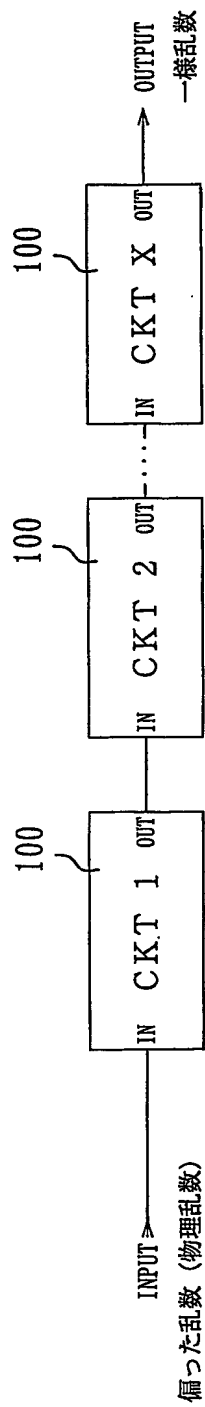


FIG. 3B

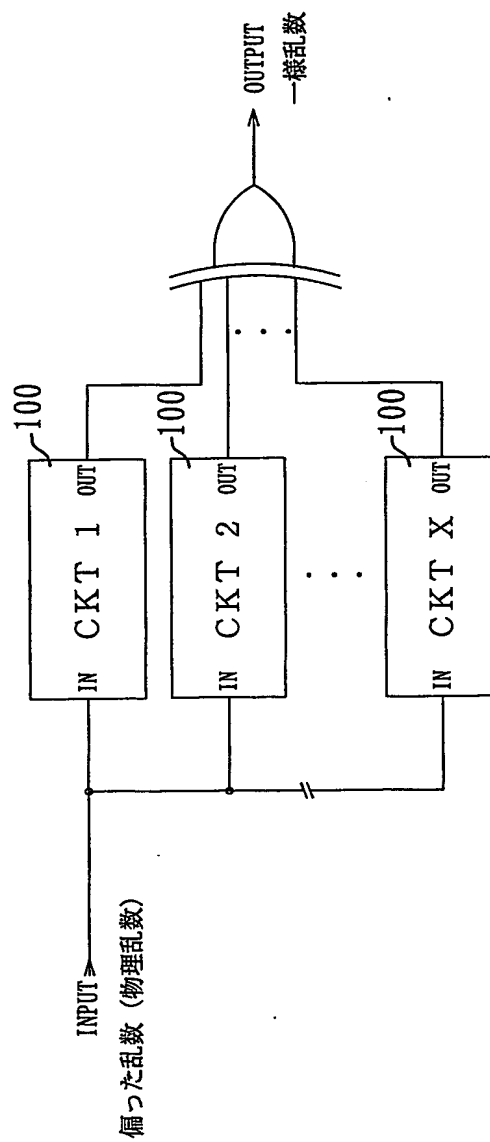


FIG. 4

91

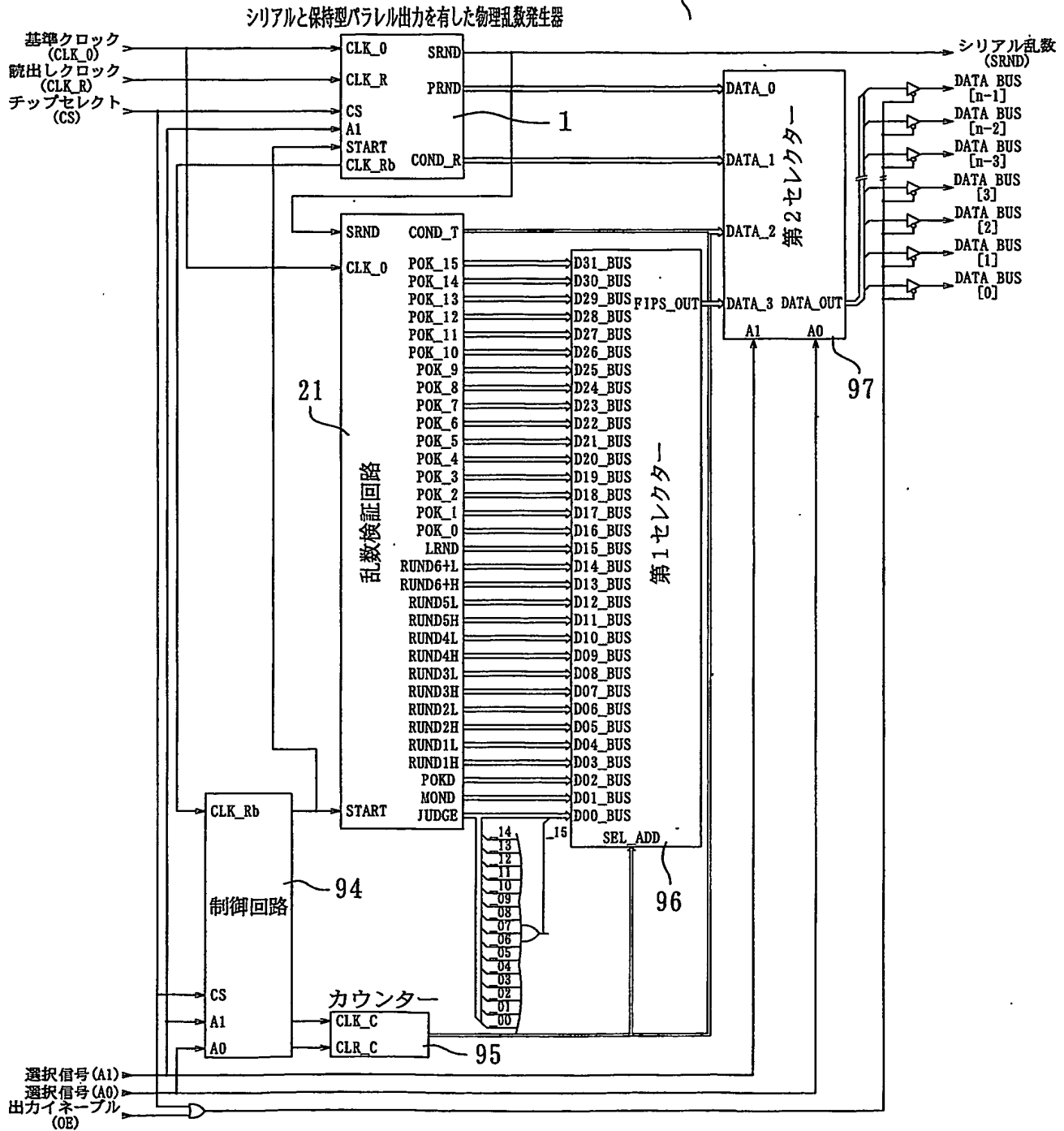


FIG. 5

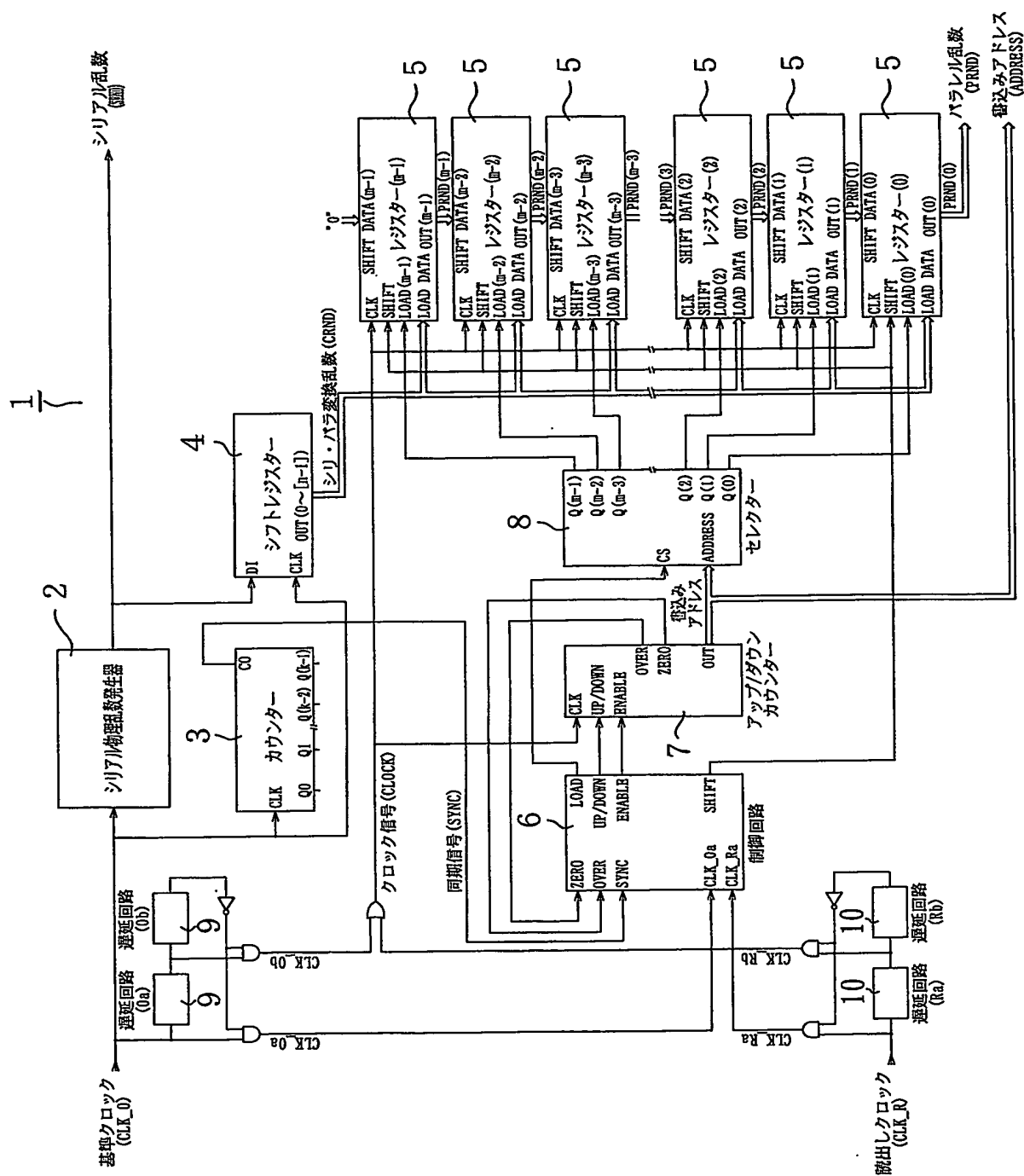


FIG. 6

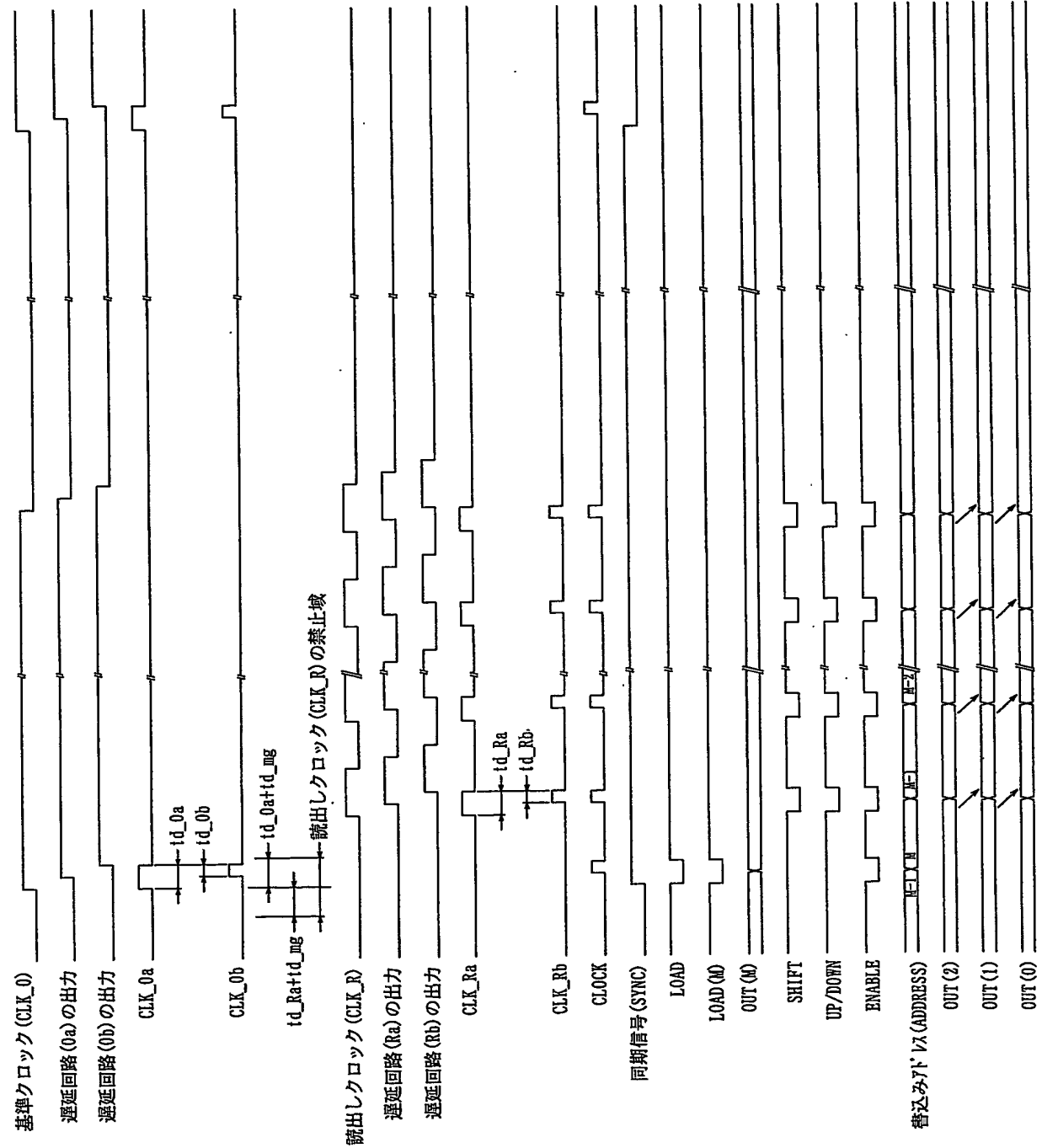


FIG. 7

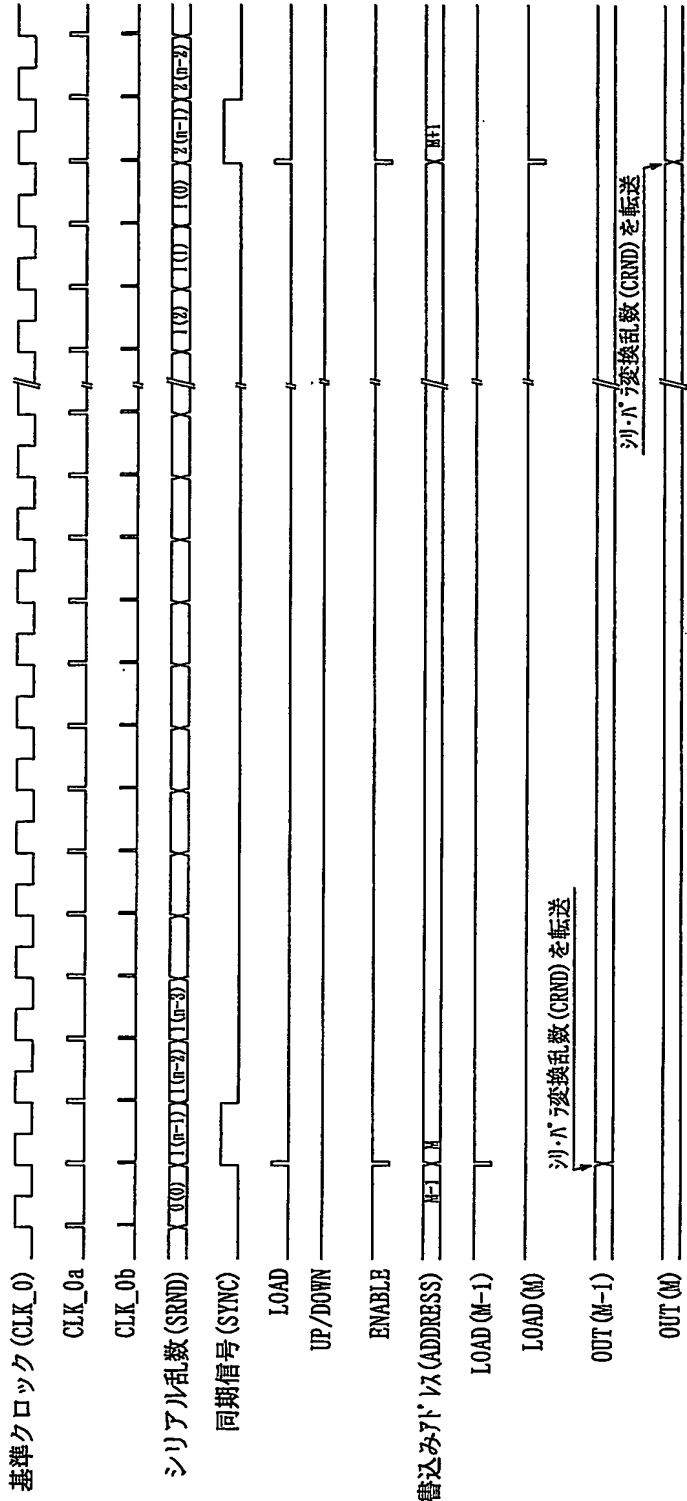


FIG. 8

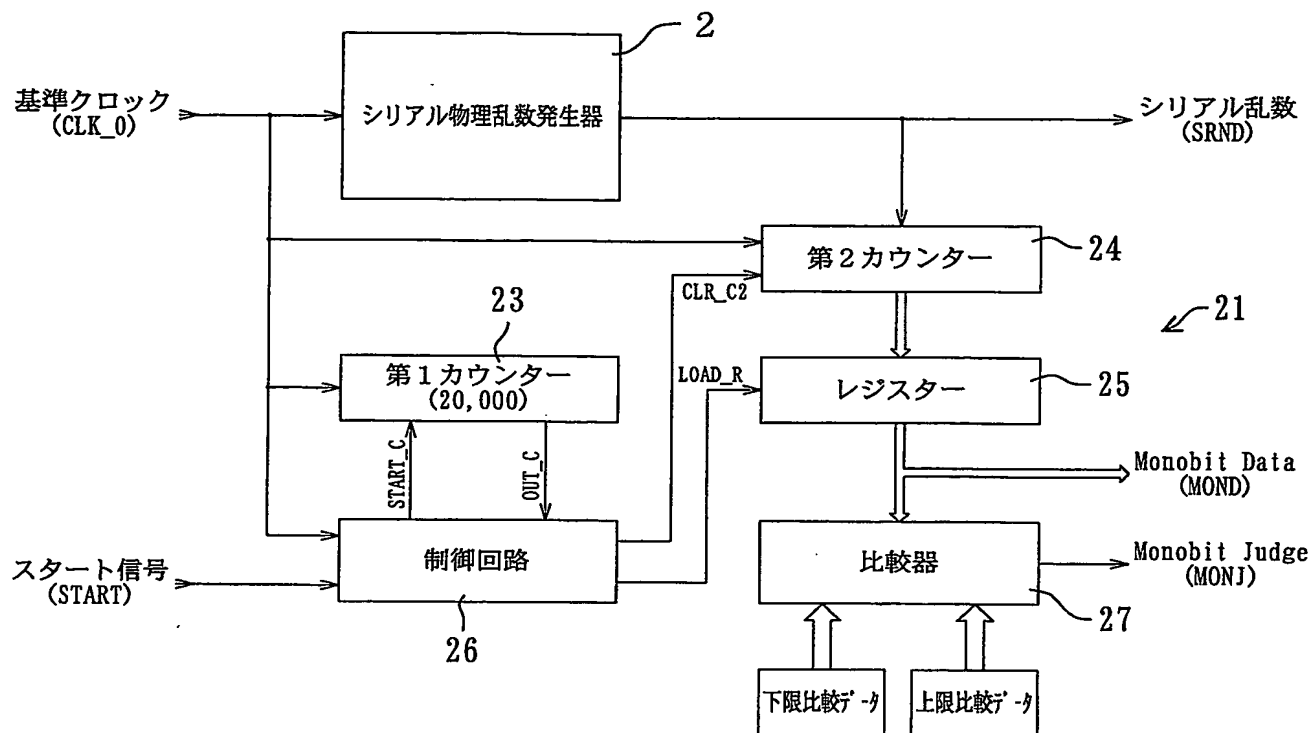


FIG. 9

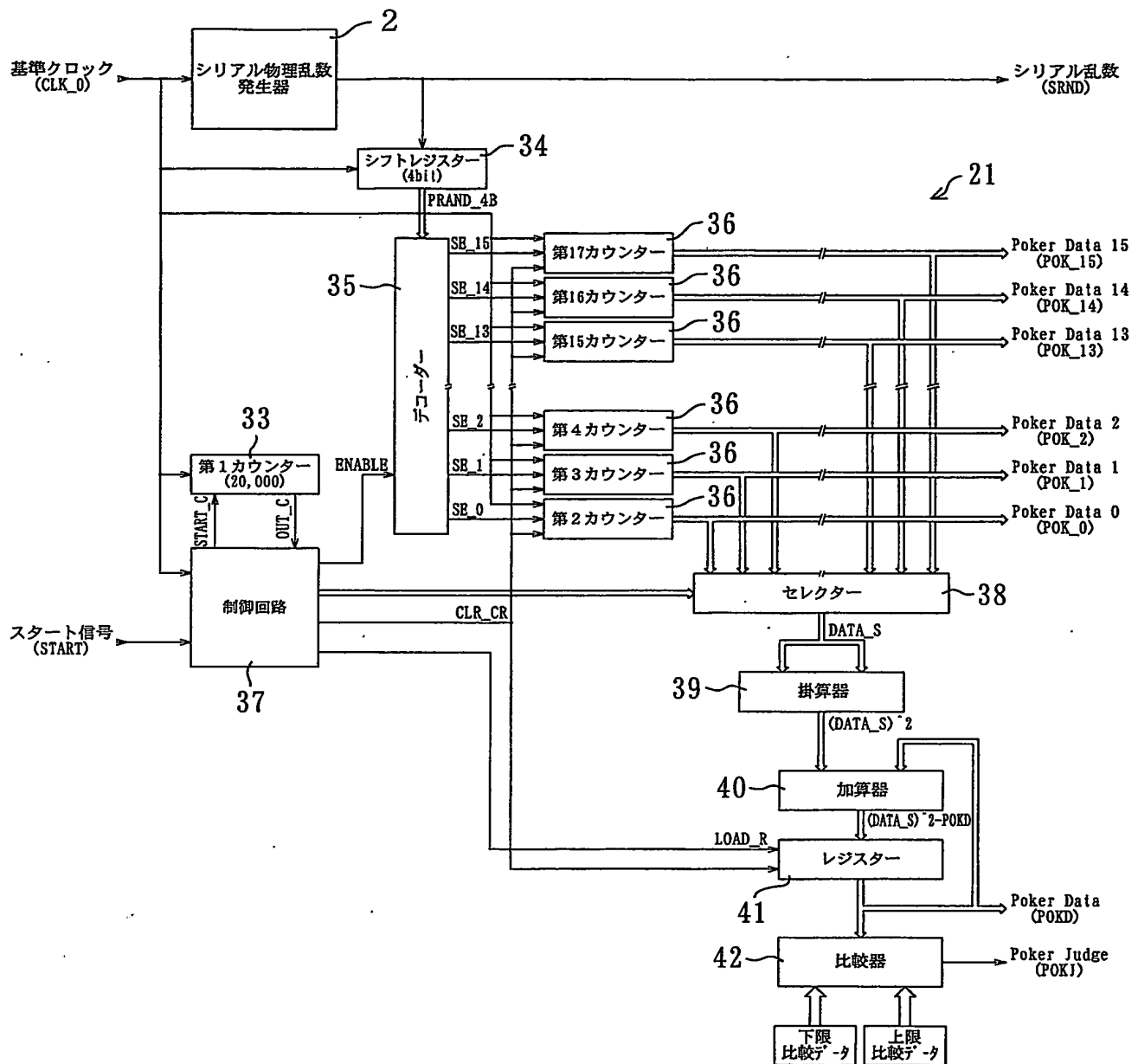


FIG. 10

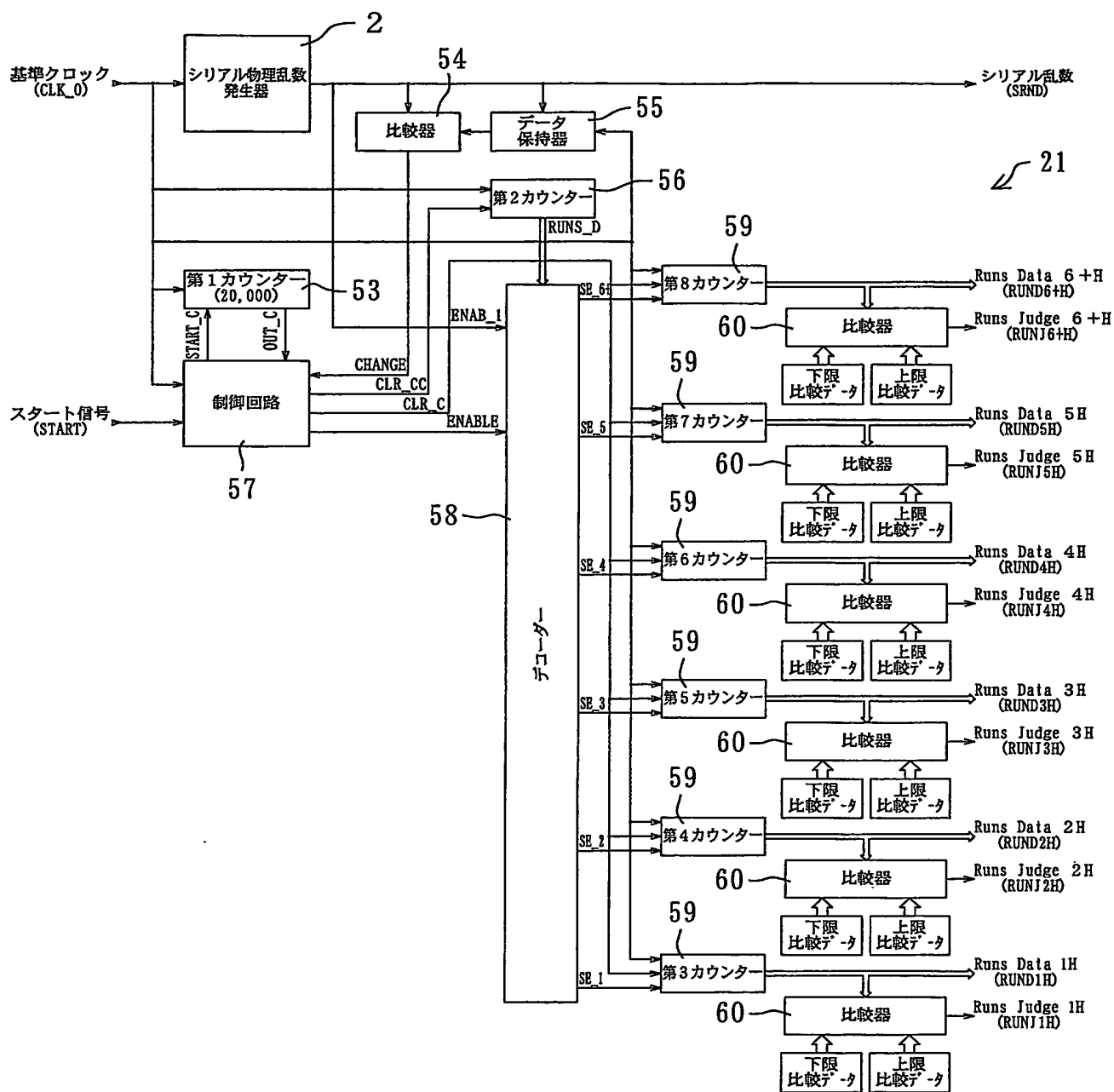


FIG. 11

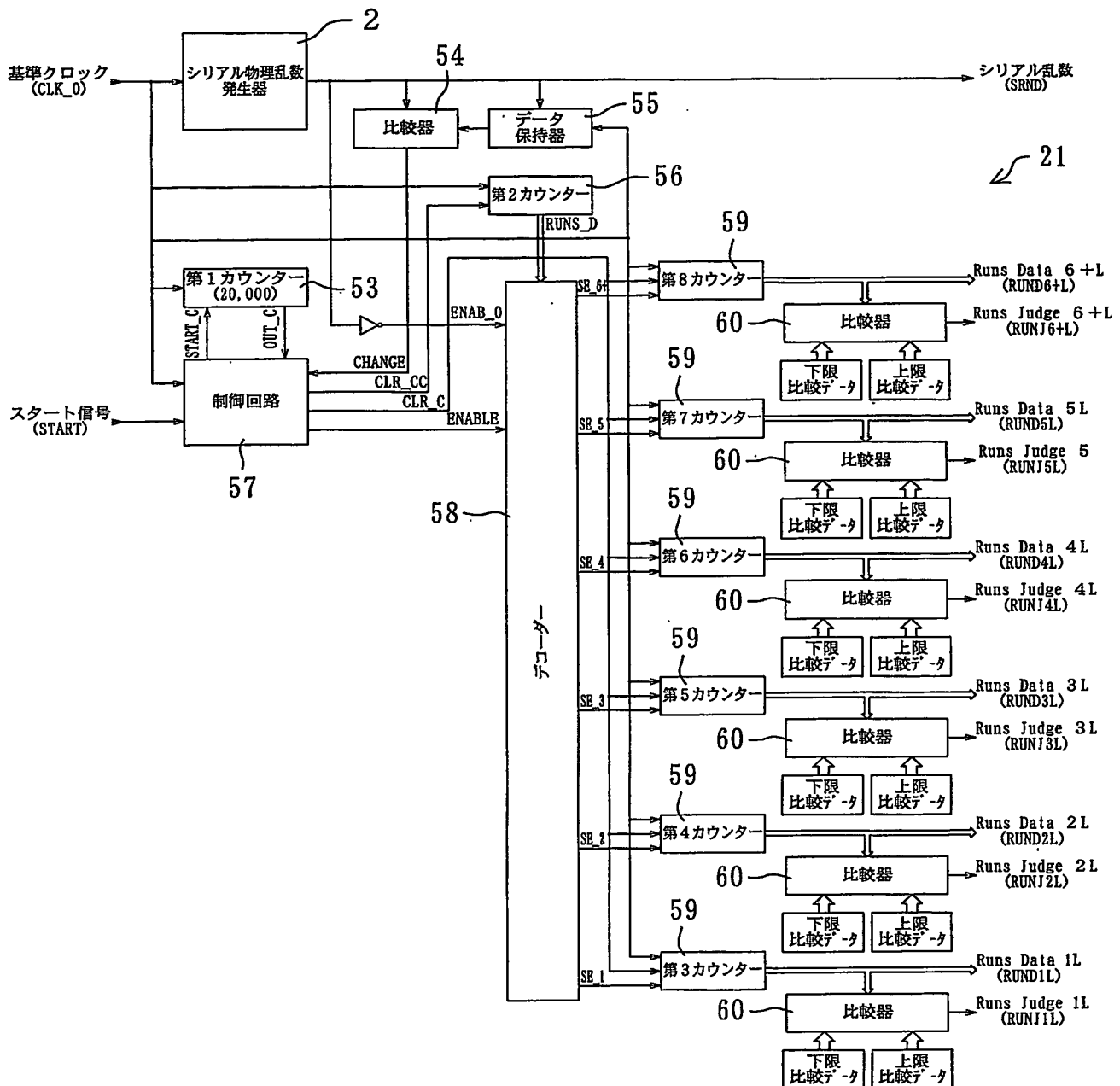


FIG. 12

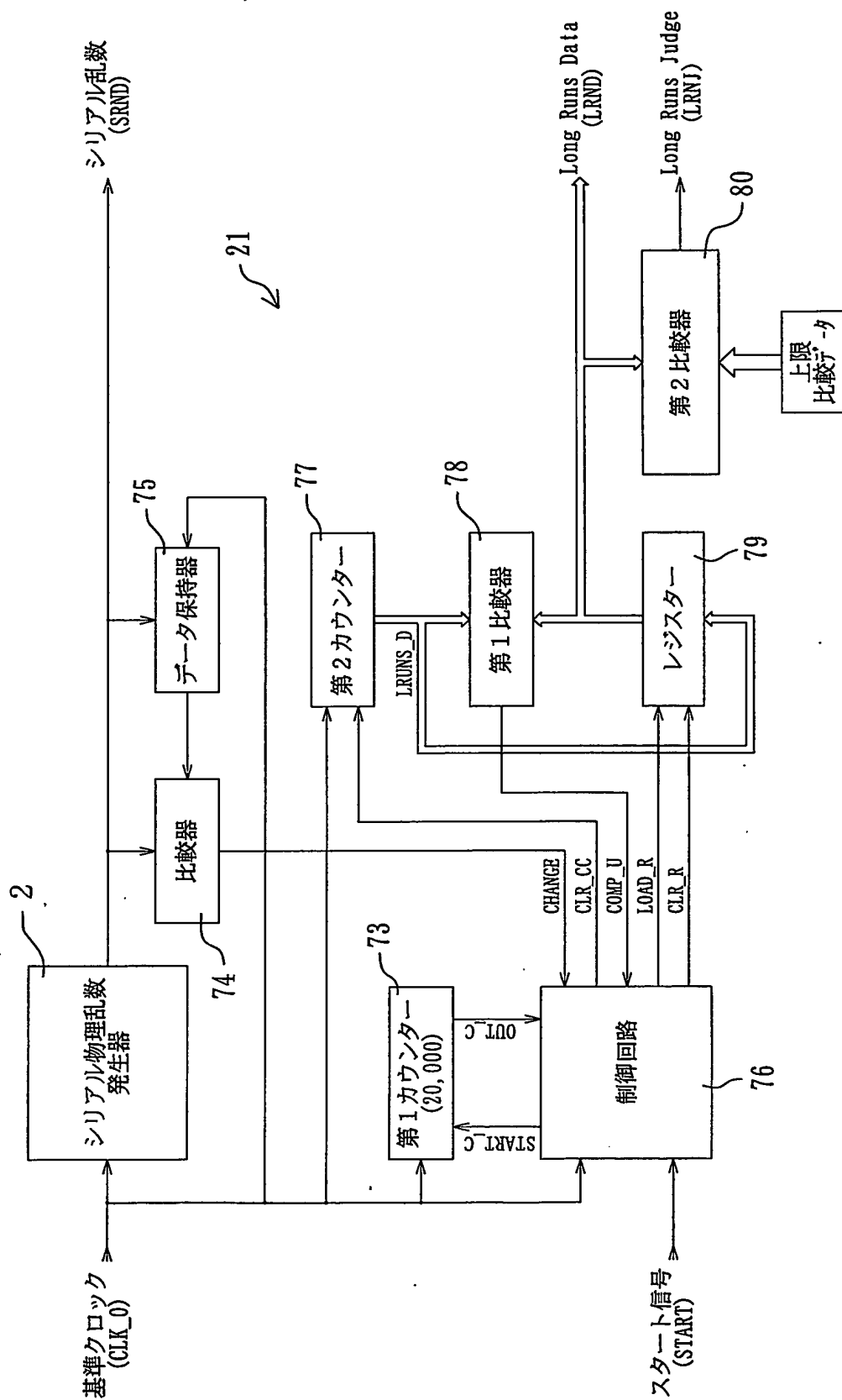


FIG. 13

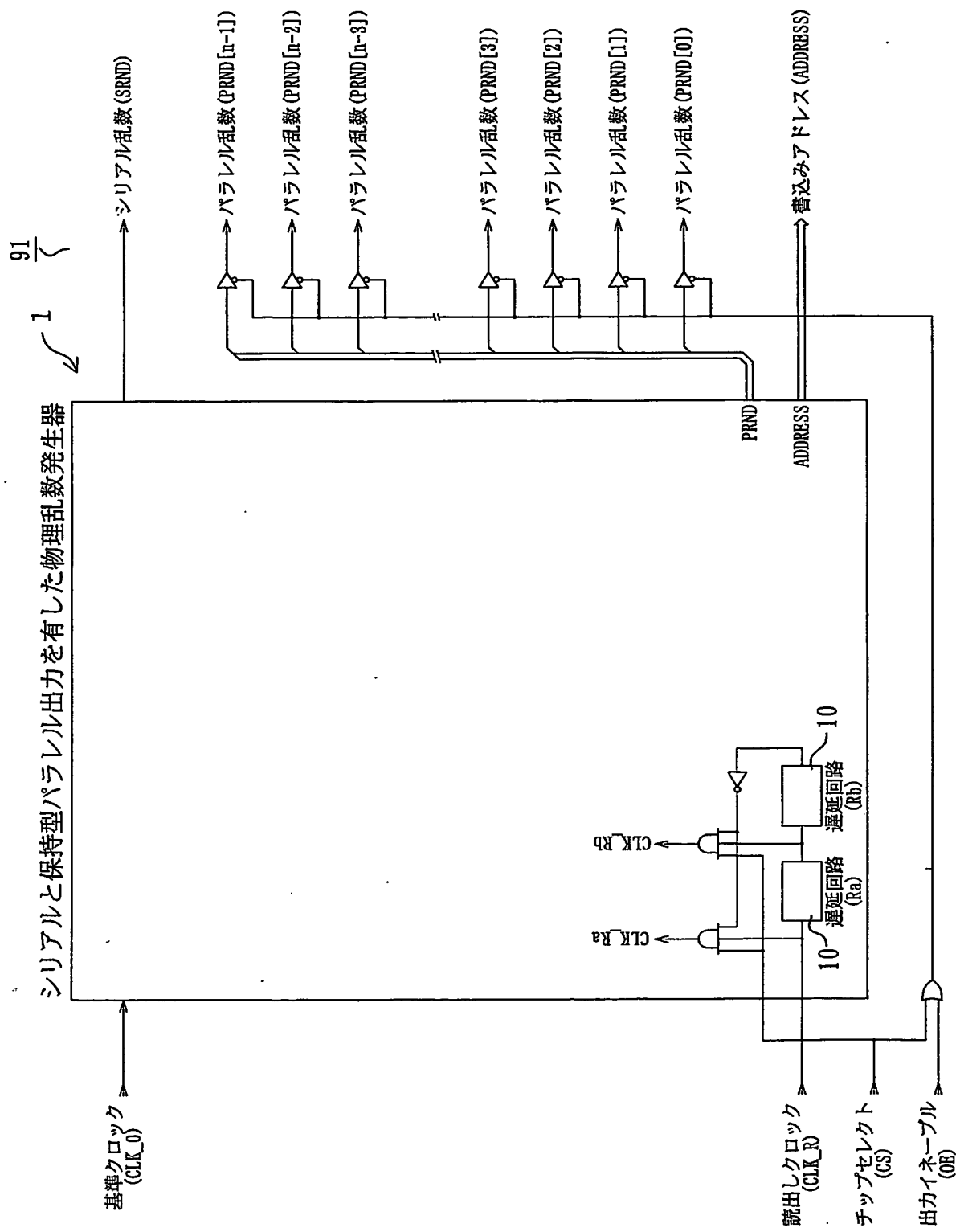


FIG. 14

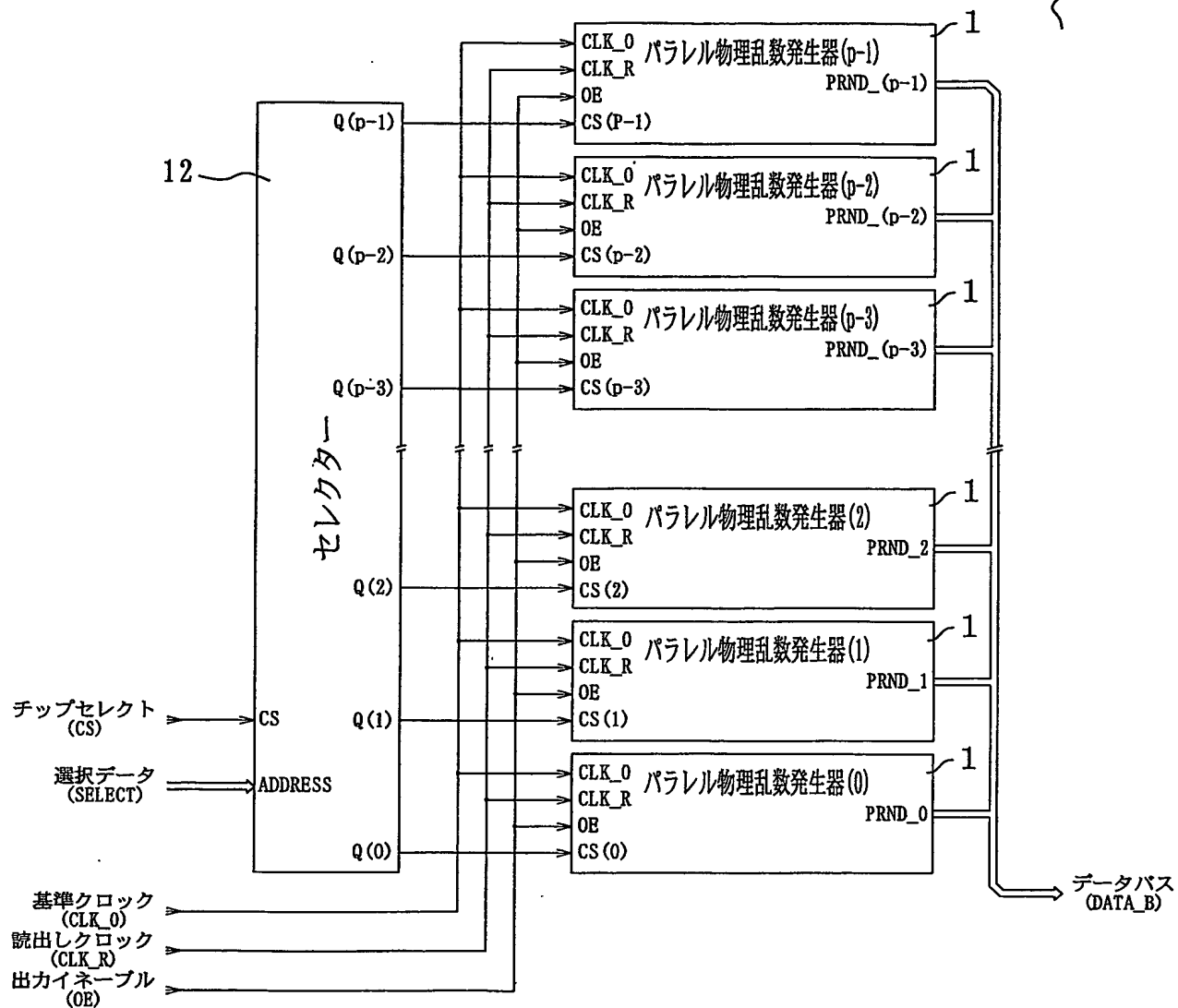
$$\frac{91}{5}$$


FIG. 15

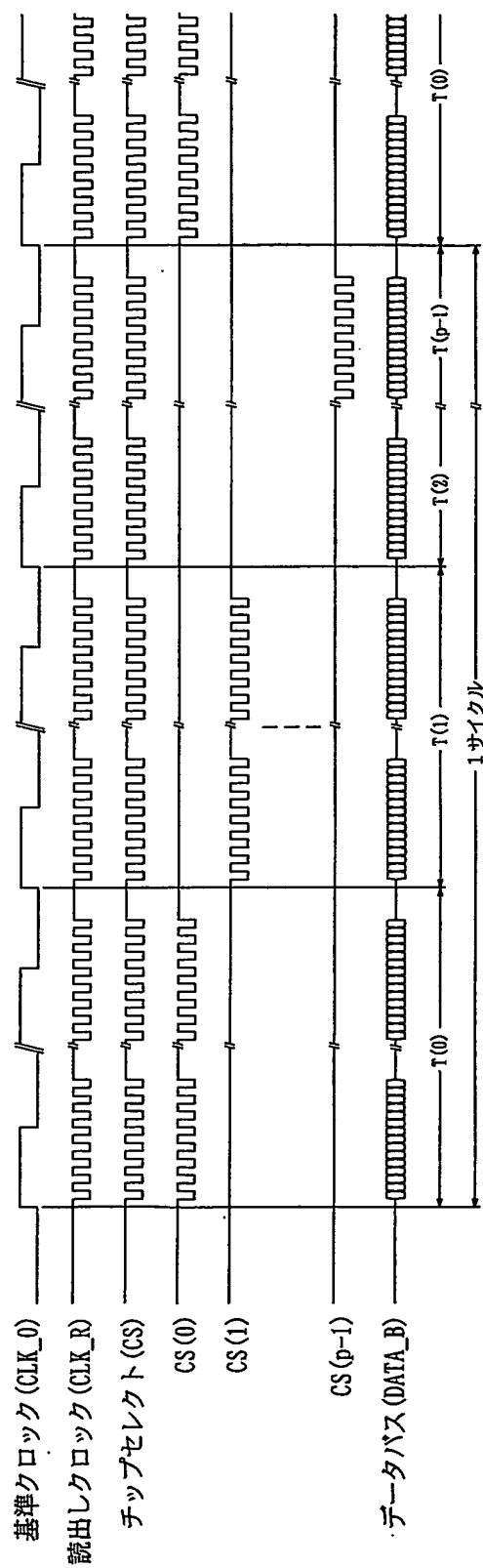


FIG. 16

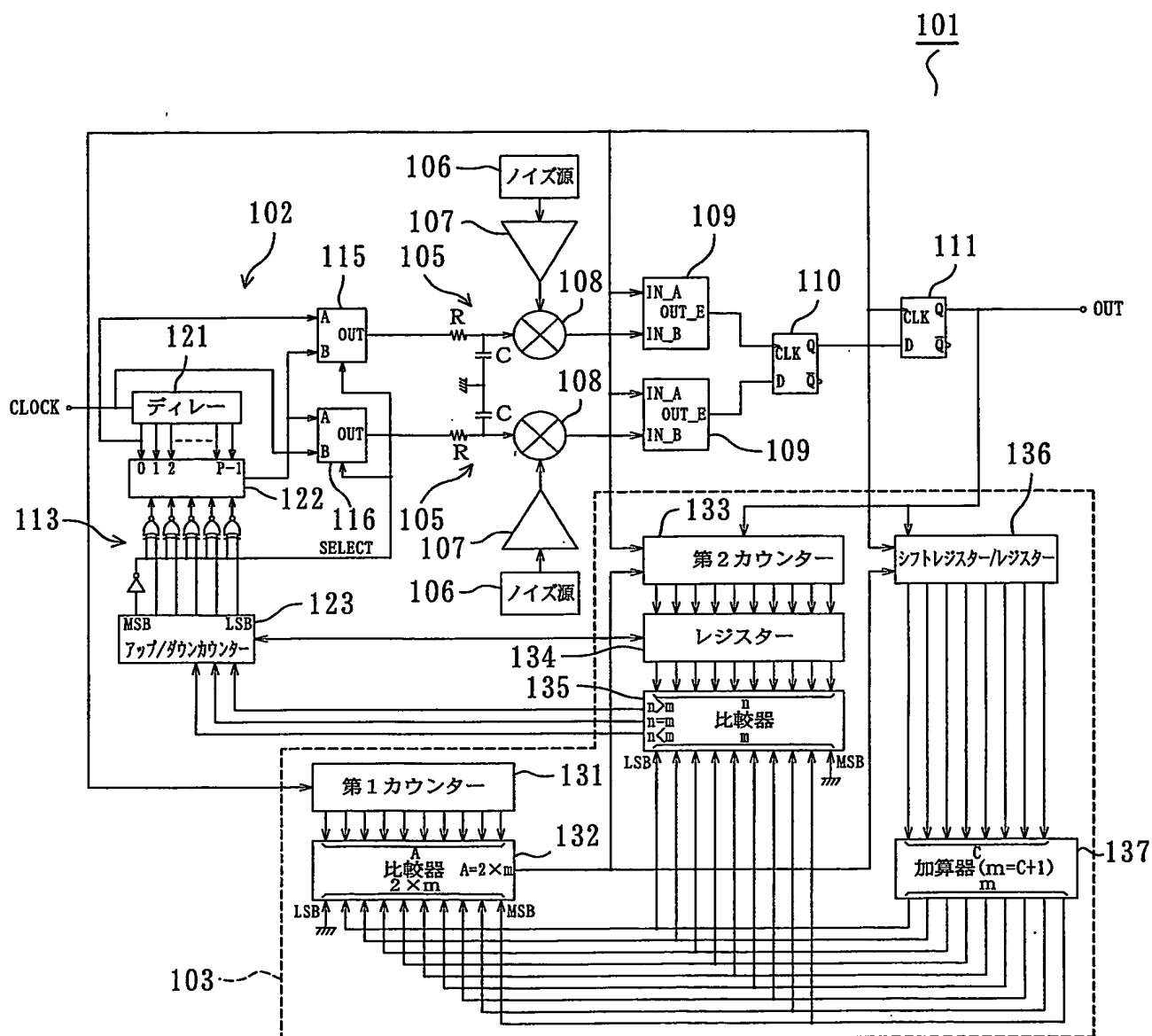


FIG. 17

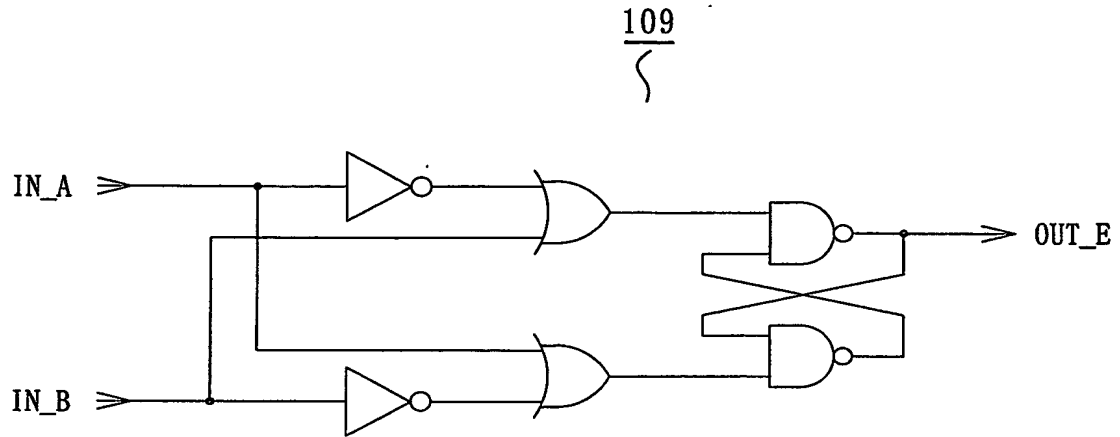


FIG. 18

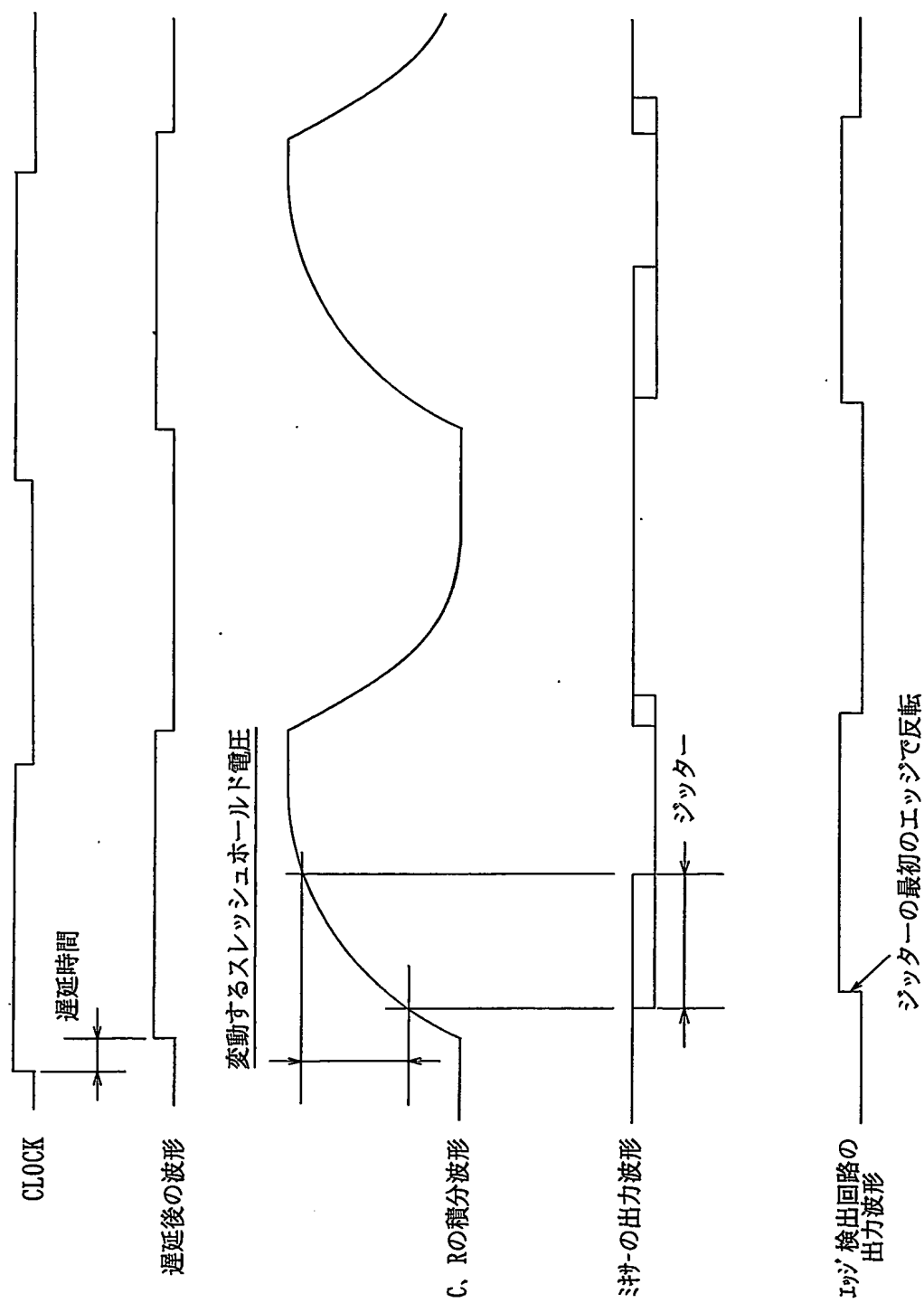


FIG. 19

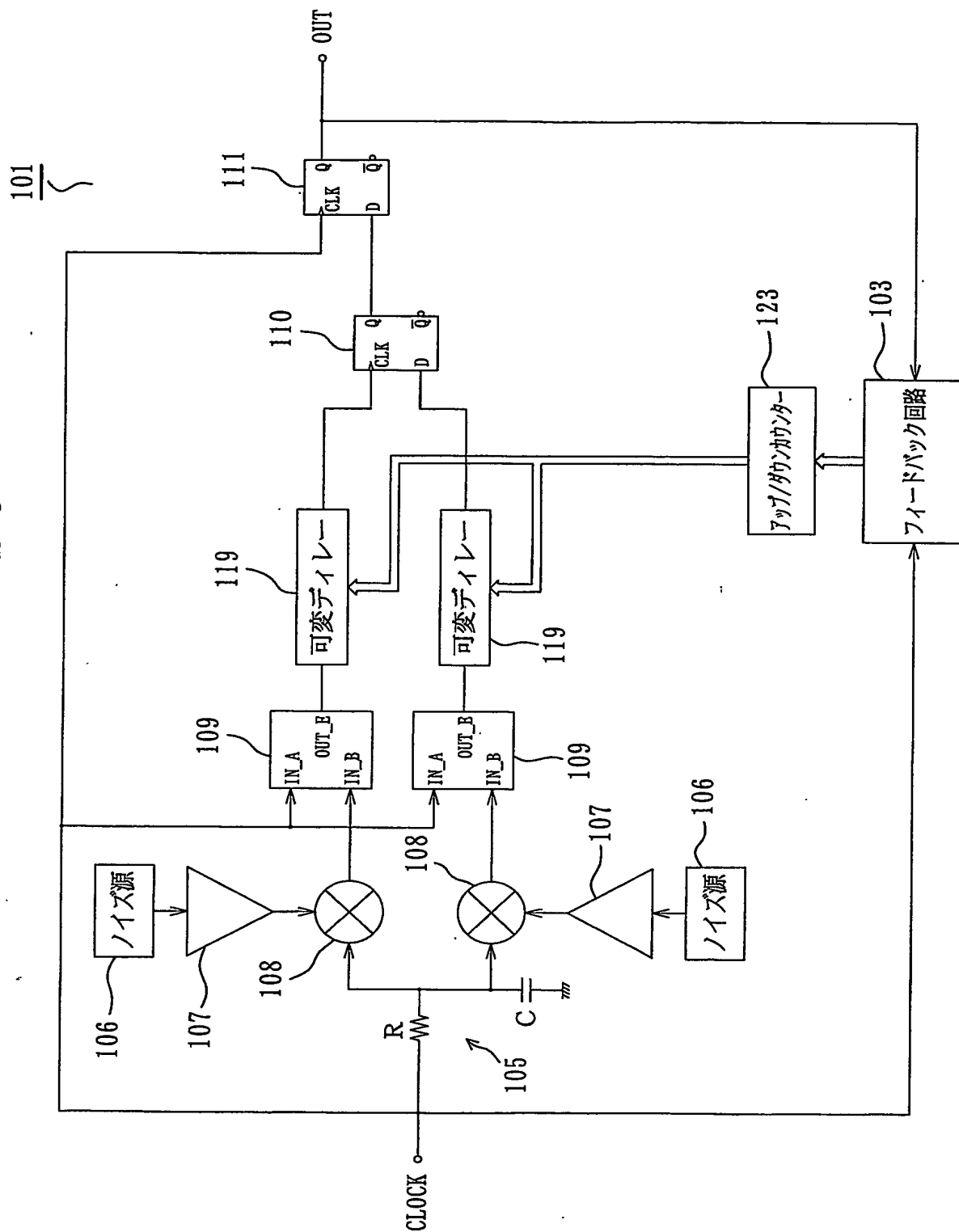


FIG. 20

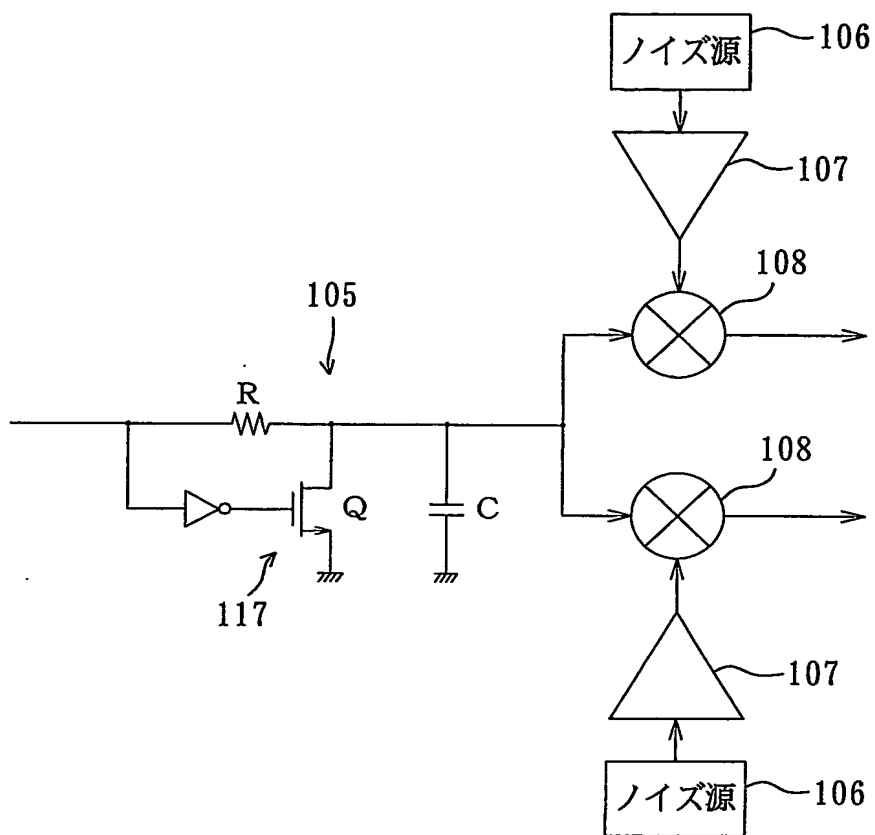


FIG. 21

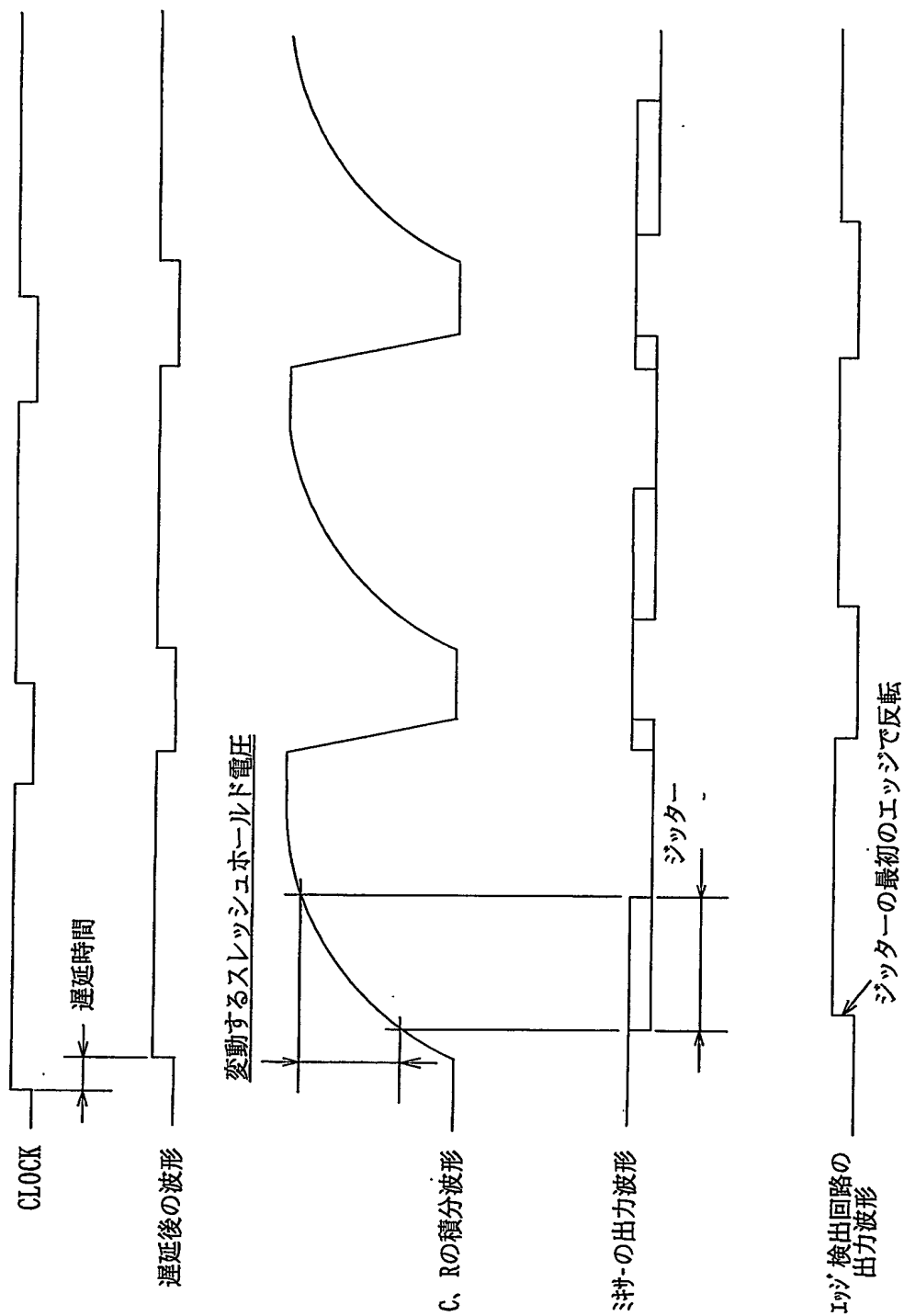


FIG. 22

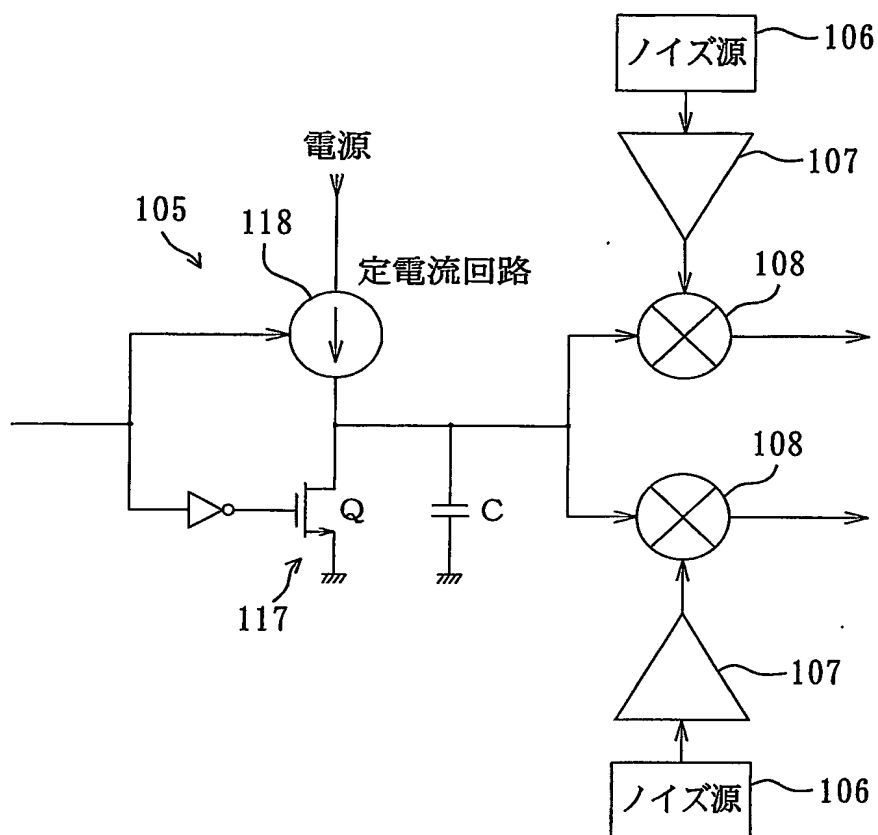
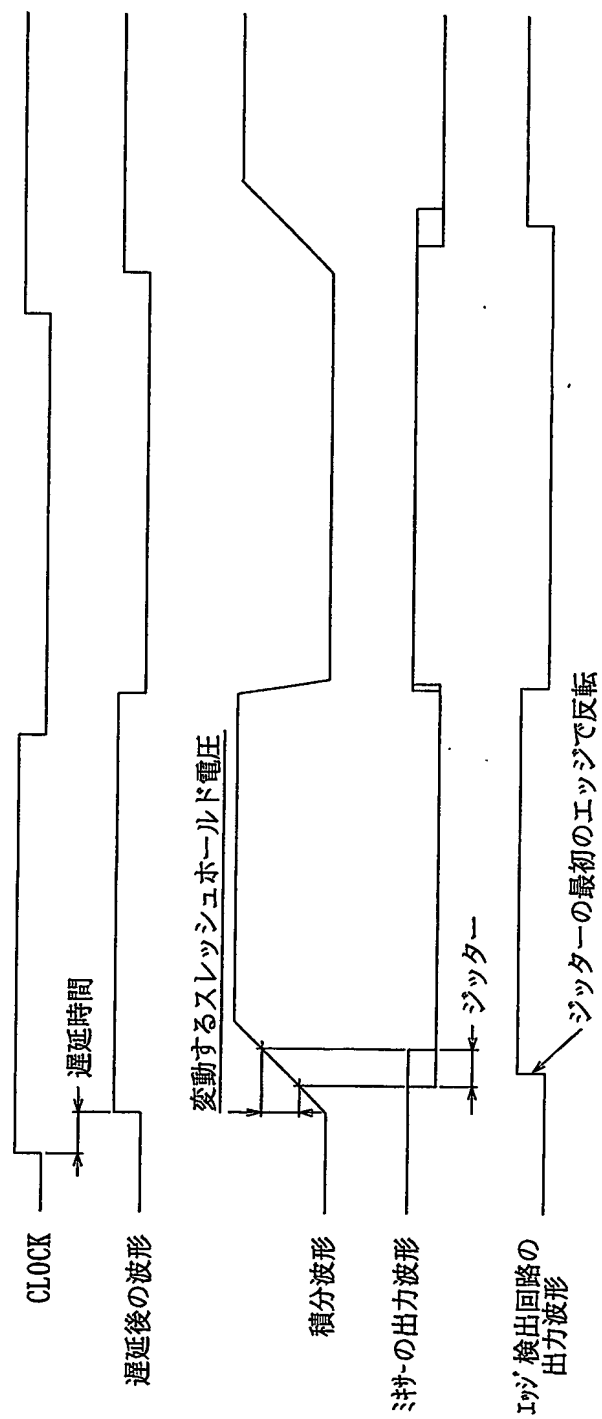


FIG. 23



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/12213

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F7/58, H03K3/84Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 62-109082 A (NEC Corp.), 20 May, 1987 (20.05.87), Full text; all drawings (Family: none)	1-5
Y	JP 1-258130 A (Matsushita Electric Industrial Co., Ltd.), 16 October, 1989 (16.10.89), Full text; all drawings (Family: none)	1-5
A	JP 8-18550 A (NTT Mobile Communications Network Inc.), 19 January, 1996 (19.01.96), Full text; all drawings & EP 680172 A2 & US 5506516 A1	1-5

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
19 December, 2003 (19.12.03)Date of mailing of the international search report
13 January, 2004 (13.01.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12213

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 61-97746 A (International Business Machines Corp.), 16 May, 1986 (16.05.86), Full text; all drawings & EP 178432 A2 & US 5046036 A1	1-5
A	JP 9-97170 A (Nikoo-Electronics Co., Ltd.), 08 April, 1997 (08.04.97), Full text; all drawings (Family: none)	6-14
P,A	JP 2003-93620 A (Iwaki Electronics Co., Ltd.), 02 April, 2003 (02.04.03), Full text; all drawings (Family: none)	6-14
P,A	JP 2003-29963 A (FDK Corp.), 31 January, 2003 (31.01.03), Full text; all drawings & WO 02/063767 A1 & CN 1397871 A	9-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12213

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 15-19
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

No sufficient mention corresponding to the claims is made in the description.

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-5 relate to a technique of using part of physical random numbers as the addresses of a selector to uniform physical random numbers.

Claims 6-14 relate to a physical random number generation device that outputs parallel random numbers by means of a plurality of registers and control circuits.

Claim 15 and 16-19 relate to a physical random number generator that generates physical random numbers by using an integrating circuit, a noise source, and an amplifier or the like.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ¹ G06F 7/58		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ¹ G06F 7/58 H03K 3/84		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2003年 日本国登録実用新案公報 1994-2003年 日本国実用新案登録公報 1996-2003年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 62-109082 A (日本電気株式会社) 1987. 05. 20, 全文、全図 (ファミリー無し)	1-5
Y	JP 1-258130 A (松下電器産業株式会社) 1989. 10. 16, 全文、全図 (ファミリー無し)	1-5
A	JP 8-18550 A (エヌ・ティ・ティ移動通信網株式会社), 1996. 01. 19, 全文、全図 & EP 680172 A2 & US 5506516 A1	1-5
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		
の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	国際調査報告の発送日	
19. 12. 03	13.01.04	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 山崎 慎一	5E 9174
	電話番号 03-3581-1101 内線 3520	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 61-97746 A (インターナショナル・ビジネス・マ シーンズ・コーポレーション) 1986. 05. 16, 全文、全図 & EP 178432 A2 & US 5046036 A1	1-5
A	JP 9-97170 A (ニコー電子株式会社) 1997. 04. 08, 全文、全図 (ファミリー無し)	6-14
PA	JP 2003-93620 A (いわき電子株式会社) 2003. 04. 02, 全文、全図 (ファミリー無し)	6-14
PA	JP 2003-29963 A (エフ・ディー・ケイ株式会社) 2003. 01. 31, 全文、全図 & WO 02/063767 A1 & CN 1397871 A	9-12

第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (PCT 17 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☒ 請求の範囲 15-19 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
明細書には、上記請求の範囲に対応する十分な記述がない。
3. ☐ 請求の範囲 _____ は、従属請求の範囲であって PCT 規則 6.4(a) の第 2 文及び第 3 文の規定に従って記載されていない。

第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲 1～5 は、物理乱数の一部をセレクターのアドレスとして使用して、物理乱数を一様化する手法に関するものである。

請求の範囲 6～14 は、パラレル乱数を複数のレジスター及び制御回路によって出力する物理乱数発生装置に関するものである。

請求の範囲 15 及び 16～19 は、物理乱数を積分回路、ノイズ源及び増幅器等を用いて生成する物理乱数発生器に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。